Fachbereich III Informations- und Kommunikationswissenschaften

Institut für Angewandte Sprachwissenschaft

MAGISTERARBEIT

INTERNATIONALES INFORMATIONSMANAGEMENT

E-Voting in Deutschland?
Zum Problem der Stimmabgabe über das Internet bei politischen Wahlen

vorgelegt von

Anna Dopatka

(anna-dopatka@gmx.net)

Erstgutachter: Dr. Folker Caroli

Zweitgutachter: Prof. Dr. Herward Sieberg

Hildesheim, im September 2005

Zusammenfassung

Diese Magisterarbeit beschäftigt sich mit der Frage, ob und gegebenenfalls in welcher Form ein internetgestütztes Wahlsystem bei politischen Wahlen in Deutschland eingesetzt werden könnte oder sollte. Hierfür ist es erforderlich, die Funktionen und Bedeutung der Wahl in der Demokratie sowie ihre verfassungsrechtliche Verankerung darzustellen. Ferner werden die Potentiale des Internets im politischen Willensbildungsprozess erörtert, indem explizit auf die neuen Informations-, Kommunikations- und Partizipationsfunktionen eingegangen wird. Die Diskussion um eine mögliche Einführung eines verfassungskonformen E-Voting-Systems bedingt ferner die Erörterung sicherheitstechnischer sowie demokratietheoretischer Anforderungen. Aufbauend auf den Ergebnissen einiger E-Voting-Pilotprojekte in In- und Ausland sind eventuelle Auswirkungen sowohl auf den Wahlprozess als auch auf die Wahlbevölkerung zu diskutieren. Diese Auswirkungen werden schließlich in Beziehung zu den in Deutschland wichtigen rechtlichen und gesellschaftlichen Rahmenbedingungen gesetzt, bevor verschiedene Einführungsmodelle entwickelt werden.

Schlagwörter: E-Voting, E-Demokratie, E-Government, politische Wahlen, Wahlrechtsgrundsätze, Datensicherheit, digitale Spaltung.

Abstract

This M.A. thesis deals with the question whether an internet-based voting system should be adopted in Germany. Starting with the meaning and functions of elections in a democratic system as well as their way of being laid down in the constitution and based on that the democratic potential of the internet is discussed. Furthermore it is necessary to explicate the new possibilities of information, communication and participation, which are offered by the medium internet. A detailed discussion about a practical adoption of a constitutional e-voting-system needs both the definition of safety regulations and democratic standards. The possible effects on the election-process itself and furthermore on the elective population are based on the results of different national and international e-voting-pilots. Conclusions drawn from those effects have to be related to determining factors like legal and social frameworks, before different schemes of adoption can be developed.

Keywords: E-Voting, E-Democracy, E-Government, political elections, suffrage, data security, digital divide.

Inhaltsverzeichnis

0 Einleitung ... 1

1 Demokratie, Wahlen und Internet ... 3

1.1 Wahlen als wesentliche Grundlage des demokratischen Systems ... 3

1.1.1 Wahlen – Funktionen und Bedeutung ... 3

1.1.2 Grundsätze von Wahlen und Abstimmungen nach dem Grundgesetz ... 8

1.1.2.1 Wahlen ... 8

1.1.2.2 Abstimmungen ... 11

1.2 Das Internet in der Demokratie ... 12

1.2.1 E-Government und E-Demokratie: eine Definition ... 12

1.2.2 Funktionen des Internets für die Demokratie ... 14

1.2.2.1 Informationsfunktion ... 14

1.2.2.2 Kommunikations- und Partizipationsfunktion ... 17

2 Anforderungen an Internet-Wahlen ... 22

2.1 Bislang diskutierte Erwartungen an das E-Voting ... 22

2.2 Eingrenzende Definitionen von E-Voting-Systemen ... 24

2.3 Demokratietheoretische Anforderungen ... 25

2.3.1 Allgemeine Wahl ... 25

2.3.2 Unmittelbare Wahl ... 29

2.3.3 Freie Wahl ... 30

2.3.4 Gleiche Wahl ... 34

2.3.5 Geheime Wahl ... 38

2.4 Sicherheitstechnische Anforderungen ... 41

2.4.1 Grundproblem Internetsicherheit ... 41

2.4.2 Angreifer und Angriffsformen ... 44

2.4.2.1 Denial-of-Service-Angriff (DoS) ... 44

2.4.2.2 Malware ... 45

2.4.2.2.1 Computerviren ... 46

2.4.2.2.2 Trojanische Pferde ... 47

2.4.2.2.3 Würmer ... 47

2.4.2.3 Spoofing 48
2.4.2.4 Man-in-the-Middle-Angriff 49
2.4.3 Technische Schutzmöglichkeiten 49
2.4.3.1 Kryptographie 50
2.4.3.1.1 Symmetrische Verschlüsselungsverfahren 51
2.4.3.1.2 Asymmetrische Verschlüsselung 52
2.4.3.1.3 Elektronische Signatur 53
2.4.3.1.4 Zertifizierungsstellen 55
2.4.3.2 Anonyme Kommunikationskanäle 57
2.4.3.3 Blinde Signaturen 58
2.4.3.4 Sicherheit des Clients 59
2.4.3.5 Sicherheit des Wahlservers 60
2.4.3.5.1 Firewalls 60
2.4.3.5.2 Maßnahmen gegen Denial-of-Service-Angriffe 60
2.4.3.5.3 Technisches Audit 62
2.4.3.5.4 Digitale Gewaltenteilung 62
2.4.4 Skizzierung eines Wahlsystems 63

3 Ergebnisse von E-Voting-Pilotprojekten bei politischen Wahlen und Abstimmungen 67
3.1 Schweiz 67
3.2 Großbritannien 71
3.2.1 St Albans 71
3.2.2 Swindon 74
3.3 Estland 76
3.4 Initiativen und Forschung in Deutschland 80
3.4.1 Forschungsgruppe Internetwahlen/ Wählen in elektronischen Netzwerken (W.I.E.N.) 80
3.4.2 Weitere Pilotprojekte 83

4 Auswirkungen von Internetwahlen – erste Erfahrungen und Annahmen 85
4.1 Finanzieller Aufwand 85
4.2 Verlust der Wahlsymbolik 88

4.2.1 Öffentlichkeit ... 88
4.2.2 Geschwindigkeit ... 89
4.2.3 Vertrauen in E-Voting als ‚sicheres Wahlverfahren' ... 91
4.3 E-Voting als Mittel zur Steigerung der Wahlbeteiligung ... 95

5 E-Voting in Deutschland? ... 100
5.1 Umgang mit dem Problem der digitalen Spaltung ... 100
5.1.1 Verbreitung und Nutzung des Internets ... 100
5.1.2 Mögliche Auswirkungen der digitalen Spaltung auf das E-Voting ... 101
5.1.3 Vorschläge zur Minderung der digitalen Spaltung ... 103
5.2 Ausbau der Public Key Infrastruktur ... 104
5.3 Änderungsbedarf des Wahlrechts ... 106
5.4 Einführungsmodelle des E-Votings ... 107
5.4.1 E-Voting im Wahllokal ... 109
5.4.2 E-Voting außerhalb des Wahllokals ... 110

6 Resümee ... 112

Literaturverzeichnis ... 116
Abbildungsverzeichnis ... 133
Eigenständigkeitserklärung ... 134

0 Einleitung

Auf dem Kongress ‚Internet - eine Chance für die Demokratie' im Mai 2001 in Berlin formuliert Bundesinnenminister Otto Schily als Fernziel, politische Wahlen über das Internet bis 2006 Realität werden zu lassen:

> „Bevor wir bei Bundeswahlen die Stimmabgabe vom heimischen PC oder per Handy anvisieren, sollten wir als ersten Schritt die Wahllokale so vernetzen, dass die Wählerinnen und Wähler nicht mehr nur in dem Wahlbezirk, in dem ihre Wohnung liegt, wählen gehen können. Es sollte ihnen ermöglicht werden, ihre Stimme in jedem beliebigen Wahllokal abzugeben. Dies trägt zur Vertrauensbildung bei. Das Ziel ist, diese Form des Wählens bei der Bundestagswahl 2006 anzubieten" [Schily 2001, 6f.].

Die angestrebte Entwicklung in Deutschland konnte bislang nicht verwirklicht werden. Dies mag auch auf den durch die vorgezogene Neuwahl im September 2005 verkürzten Zeitrahmen zurückzuführen sein. Insbesondere jedoch verdeutlichten bislang durchgeführte Initiativen und Pilotprojekte, dass die Einführung eines E-Voting-Systems nicht lediglich eine Erweiterung der technischen Möglichkeiten zur Stimmabgabe bedeutet. Es sind vielmehr weitreichende rechtliche, sicherheitstechnische und organisatorische Fragen zu beantworten und Regelungen zu schaffen.

Die Erwartungen der Öffentlichkeit an das E-Voting variieren deutlich. Auf der Seite der Befürworter steht euphorische Hoffnung auf eine umfassende Erneuerung der Demokratie durch Betonung der direktdemokratischen Elemente mittels des Internets. Kritiker dagegen fürchten um die Sicherheit der Wahlrechtsgrundsätze und erwarten durch Verlegung der Wahl aus der Öffentlichkeit in den privaten Raum eine Entwertung der Demokratie.

Um die Frage beantworten zu können, ob und gegebenenfalls unter welchen Bedingungen ein E-Voting-System in Deutschland eingeführt werden könnte und sollte, erfolgt im ersten Kapitel zunächst die Darstellung von Funktionen und Bedeutungen einer demokratischen Wahl sowie ihre verfassungsrechtliche Verankerung. Anschließend werden die Potentiale des Internets in der Demokratie erörtert, indem explizit auf die neuen Informations-, Kommunikations- und Partizipationsmöglichkeiten im politischen Willensbildungsprozess eingegangen wird.

Im zweiten Kapitel werden nach einer Darstellung der bislang diskutierten Erwartungen an Internetwahlen und einer Abgrenzung der verschiedenen Typologien sodann die An-

forderungen an Internetwahlen diskutiert, sowohl auf demokratietheoretischer als auch auf sicherheitstechnischer Ebene.

Aufbauend auf den im dritten Kapitel vorgestellten Ergebnissen der Pilotprojekte und Forschungsinitiativen in In- und Ausland erfolgt im vierten Kapitel eine Einschätzung der Auswirkungen von Wahlen im Internet. Dies bezieht sich einerseits auf eventuelle Rationalisierungsmöglichkeiten bezüglich der Kosten, andererseits auf die Wahlbevölkerung. Das traditionelle Wahlverfahren genießt weitreichendes Vertrauen unter den Bürgern und hat sich als ‚sicheres' Wahlverfahren etabliert. Durch die Virtualisierung des wichtigsten Legitimationsmodus' der Regierenden kann ein Verlust der Wahlsymbolik entstehen, der sich wiederum negativ auf das Vertrauen der Bevölkerung in den demokratischen Akt der Wahl auswirken könnte. Andererseits stellt sich die Frage, ob die Internetwahl auch eine Lösung für das Problem der sinkenden Wahlbeteiligung darstellen könnte.

Diese möglichen Auswirkungen können durch verschiedene gesellschaftliche und rechtliche Rahmenbedingungen verstärkt bzw. relativiert werden. Im fünften Kapitel erfolgt daher die Betrachtung dieser für eine erfolgreiche Einführung des E-Votings in Deutschland wichtigen Rahmenbedingungen. Der Einfluss der ‚digitalen Spaltung' auf die virtualisierte politische Teilnahme muss dabei ebenso beachtet werden wie die Schaffung sicherheitstechnischer Infrastrukturen. Gleichzeitig ist es erforderlich, den Änderungsbedarf im Wahlrecht zu diskutieren, bevor abschließend verschiedene Einführungsmodelle vorgestellt werden können.

1 Demokratie, Wahlen und Internet

1.1 Wahlen als wesentliche Grundlage des demokratischen Systems

1.1.1 Wahlen – Funktionen und Bedeutung

Der Begriff der Wahl umfasst sowohl politische als auch nicht-politische Wahlen, wie z.B. Personalrats-, Betriebrats-, Hochschul- oder Sozialwahlen. Beide Formen sind weder zwingend an die gleichen gesetzlichen Vorgaben gebunden noch sind ihre Funktionen und Bedeutung identisch. Den Schwerpunkt dieser Arbeit bilden die politischen Wahlen.

Zu unterscheiden ist ferner zwischen politischen Wahlen und sogenannten Plebisziten. Während ‚Wahlen' die regelmäßigen Wahlen zu Volksvertretungen sind [vgl. Woyke 1998, 17], umfasst der Begriff ‚Plebiszit' Volksbegehren, Volksentscheid und Volksabstimmung, die sich hauptsächlich auf Sachentscheidungen beziehen.

Politische Wahlen haben in modernen Staatsformen zunächst eine offensichtliche Zielsetzung: die personelle Besetzung bzw. Zusammensetzung eines Staatsorgans. „Die Wahl ist die demokratische Methode der Bestellung von Personen in Vertretungsorgane oder Führungspositionen" [Nohlen 2004, 21]. Dies gilt insbesondere in Systemen, in denen die Bürger nicht direkt an allen Entscheidungen und Handlungen beteiligt sind, also in allen repräsentativen Staatsformen. In demokratischen Staatsgebilden sind die Bürger nicht direkt als Entscheidungsträger tätig. Vielmehr erfolgt eine Bündelung des politischen Willens der Wähler und seine Umsetzung durch Beauftragung der Mandatsträger auf Zeit [vgl. Schreiber 2002, 29].

Wahlen haben sich als Teil eines demokratischen Systems historisch in einem langen Prozess herausgebildet und durchgesetzt, dennoch beschränken sich Wahlen nicht nur auf Demokratien [vgl. Nohlen 2004, 21]. Die demokratischen Aspekte einer Wahl werden durch die jeweilige institutionelle Ausgestaltung des politischen Systems und durch das Wahlverfahren näher definiert [vgl. Neymanns 2002b, 24]. Die erste offizielle Postulierung der Grundgedanken zur erforderlichen Legitimität von Regierungen findet sich in der Unabhängigkeitserklärung der Vereinigten Staaten von 1776. Sie besagt, dass

> „Regierungen eingesetzt sein müssen, deren volle Gewalten von der Zustimmung der Regierten herkommen; dass zu jeder Zeit [...] das Volk das Recht hat, jene zu ändern oder abzuschaffen, eine neue Regierung einzusetzen“[1].

In Preußen wurde nach den Stein-Hardenberg'schen Reformen ab 1808 in Anlehnung an die demokratischen Verfassungsvorstellungen der Französischen Revolution ein allgemeines Wahlrecht eingeführt. Jedoch bestand dieses Recht nur für Männer und war zudem an einen Zensus gebunden [vgl. Vogt 1997, 408]. Bis 1918 das allgemeine Wahlrecht für Männer und Frauen gültig wurde, war der Zugang zum Wahlrecht im Deutschen Reich aufgrund des sozialen Status', der Religion oder des Geschlechts beschränkt. In Preußen z.B. galt seit 1849 das Dreiklassenwahlrecht, das sich nach dem Steueraufkommen richtete. Seit Ende des Nationalsozialismus' besteht im Grundgesetz[2] von 1949 eine allgemeine, unmittelbare, freie, gleiche und geheime Wahl für alle Bürger[3].

Ein nach heutigem Verständnis demokratisches Wahlsystem muss neben der Wahl als technischen Legitimationsmodus zusätzlich über eine ‚liberale Komponente' verfügen [vgl. Nohlen 2004, 22]. Aus verfassungsrechtlicher Sicht ist damit die Gewährung der Meinungs-, Presse-, Versammlungs- und Vereinigungsfreiheit[4] zu verstehen, aus verfassungspolitischer Sicht der „Pluralismus in Wettbewerb um politische Mandate und Führungspositionen stehender politischer Parteien“ [Nohlen 2004, 22]. Die Grundlage des westlich-liberalen Demokratieverständnisses bildet damit die Konkurrenztheorie, d.h. die Legitimität und Anerkennung unterschiedlicher Interessen in einem politischen Gemeinwesen [vgl. Korte 2003, 8]. Dafür muss ein Minimum an gemeinsamen gesellschaftlichen Grundüberzeugungen gegeben sein, z.B. die Anerkennung des Mehrheitsprinzips [vgl. Bundesverfassungsgerichtsentscheidung[5] 1, 299 (315); 29, 154 (165)]. Die in rechtmäßigen und freien Wahlen unterlegene Gruppe muss die politische Mehrheitsmeinung anerkennen, denn nur so können Entscheidungen in pluralistischen Gesellschaften mit unterschiedlichen, teilweise konträren Interessen gefällt werden [vgl. Hesse 1995, 63]. Kontrolliert wird das Mehrheitsprinzip durch den Minderheitenschutz. Mehrheitsentscheidungen sind nur insoweit akzeptabel, als das Recht der politischen

[1] Deutsche Version der Amerikanischen Unabhängigkeitserklärung unter www.verfassungen.de/us/unabhaengigkeit76.htm (Verifizierungsdatum: 16.09.2005).
[2] Das Grundgesetz wird im Folgenden als GG bezeichnet.
[3] Vgl. Artikel 38 GG.
[4] Vgl. Artikel 5, 8 und 9 GG.
[5] Eine Bundesverfassungsgerichtsentscheidung wird im Folgenden als BVerfGE bezeichnet.

Minderheit gesichert ist [vgl. Korte 2003, 8]. Diese ‚liberale Komponente' wird im Prinzip der Öffentlichkeit einer Demokratie verdeutlicht. Als „Herzstück des modernen Parlamentarismus" [Karpen 2005, 31] dient das Öffentlichkeitsprinzip der Transparenz, Legitimation und Kontrolle des demokratischen Rechtsstaats. Diese Öffentlichkeit ist in allen Phasen der Wahl, mit Ausnahme der eigentlichen Stimmabgabe, notwendig.

Dem Wortsinn des Begriffs der Wahl nach, muss einem Wähler die tatsächliche Wahlfreiheit und die Auswahlmöglichkeit zwischen mindestens zwei Angeboten gegeben sein. Diese Wahlmöglichkeiten dürfen jedoch nicht nur prinzipiell bestehen, sondern müssen rechtlich jedem wahlberechtigten Bürger durch aktives und passives Wahlrecht zugesichert sein. In diesem Fall spricht man von kompetitiven Wahlen [vgl. Nohlen 2004, 23]. Werden die Auswahlmöglichkeiten und die Wahlfreiheit beschränkt, handelt es sich um semi-kompetitive Wahlen. Werden sie dem Wähler gänzlich verweigert, ist die Wahl nicht-kompetitiv [vgl. ebd.].

Kompetitive Wahlen zeichnen sich in liberal-demokratischen Staatssystemen durch formelle Verfahren aus, deren Gewährleistung die Voraussetzung für die Anerkennung des Wahlergebnisses seitens der Wähler ist. Hierzu zählen der Wahlvorschlag, der Wettbewerb der Kandidaten verbunden mit der Konkurrenz politischer Programme und Parteien, die Chancengleichheit im Bereich der Wahlwerbung, die Wahlfreiheit, gesichert durch die geheime Stimmabgabe, das Wahlsystem, die Umsetzung der Wählerstimmen in Mandate und die Wahlentscheidung für die Dauer einer Wahlperiode [vgl. Nohlen 2004, 24]. Diese Prinzipien sind jedoch eher normative Eigenschaften einer liberal-pluralistischen Demokratieidee, die der Wirklichkeit nicht immer vollends entsprechen. Angesichts der Parteienwirklichkeit besteht de facto ein begrenzter Pluralismus. Die realen Verhältnisse in kompetitiven Demokratien sind dennoch nicht mit denen der nicht- oder semi-kompetitiven Wahlen in autoritären und totalitären Systemen zu vergleichen.

Kompetitive Wahlen legitimieren ein politisches System in zweifacher Hinsicht: zum einen durch den Legitimitätsanspruch der Herrschenden, der durch rechtmäßige Wahlen entsteht, zum anderen „aufgrund des Legitimitätsglaubens, der politischen Systemen zuwächst, deren politische Führung aus freien Wahlen hervorgeht" [Nohlen 2004, 25]. Die durch eine freie, gleiche und allgemeine Wahl legitimierten Volksvertreter werden in der Regel von den Wählern als nach demokratischen Grundsätzen gewählt anerkannt. Denn

> „ohne Wahlen, ohne den offenen Wettbewerb gesellschaftlicher Kräfte und politischer Gruppen um die politische Macht, keine Demokratie“ [ebd.].

Hinsichtlich der Funktionen und Bedeutungen ist festzuhalten, dass diese in direktem Zusammenhang mit den gesellschaftlichen und politischen Verhältnissen sowie der Auffassung von Staat und Gesellschaft stehen. So kann die Wahl als Vertrauensbeweis der Wähler an die Gewählten gesehen werden, als ein Akt, durch den die Bildung einer funktionsfähigen Repräsentation erfolgen soll oder als eine Kontrolle über die amtierende Regierung. Wahlen

> „üben [...] zugleich mehrere Funktionen aus, die nebeneinander bestehen und historisch in unterschiedlicher Mischung auftreten.[...] Diese Variabilität in den erreichbaren Zielfunktionen ist sicherlich eine der Bedingungen, welche es der Wahl gestattet, sich den wechselhaften Umweltbedingungen und Systemanforderungen erfolgreich anzupassen“ [Nohlen 2004, 29].

Hierzu zählen z.B. soziokulturelle und ethnische Strukturen innerhalb einer Gesellschaft. In einer heterogenen Gesellschaft gilt es, alle kulturellen und ethnischen Gruppen zu repräsentieren oder die mögliche Disharmonie unterschiedlicher Gruppierungen durch politische Mehrheitsbildung zu kontrollieren. In homogenen Gesellschaften mit stabilen demokratischen Verhältnissen ist demgegenüber primär der Wettbewerb zwischen den regierenden Parteien und der Opposition zu erhalten. Dies wird durch die Kontrollfunktion der Bevölkerung über die regierenden Parteien ergänzt. Basis dieser Kontrollfunktion ist die zeitliche Limitierung der Volksvertretung, die sowohl aus Wahlen hervorgeht und auch durch Wahlen wieder abgelöst werden kann [vgl. BVerfGE 18, 151 (154)].

Für „relativ homogene Gesellschaften ohne große Konfliktlinien“[Nohlen 2004, 30 f.], die in einer stabilen parlamentarischen Demokratie mit eher wenigen Parteien leben, können folgende Funktionen von Wahlen in einer liberalen Demokratie genannt werden:

- Legitimierung des politischen Systems und der Regierung einer Partei oder Parteienkoalition
- Übertragung von Vertrauen an Personen und Parteien
- Rekrutierung der politischen Elite
- Repräsentation von Meinungen und Interessen der Wahlbevölkerung
- Verbindung der politischen Institution mit den Präferenzen der Wählerschaft

- Mobilisierung der Wählerschaft für gesellschaftliche Werte, politische Ziele und Programme, parteipolitische Interessen
- Hebung des politischen Bewusstseins der Bevölkerung durch Verdeutlichung der politischen Probleme und Alternativen
- Kanalisierung politischer Konflikte in Verfahren zu ihrer friedlichen Beilegung
- Integration des gesellschaftlichen Pluralismus und Bildung eines politisch aktionsfähigen Gemeinwillens
- Herbeiführung eines Konkurrenzkampfes um politische Macht auf der Grundlage alternativer Sachprogramme
- Herbeiführung einer Entscheidung über die Regierungsführung in Form der Bildung parlamentarischer Mehrheiten
- Einsetzung einer kontrollfähigen Opposition
- Bereithaltung des Machtwechsels

[vgl. ebd.]

Besondere Bedeutung ist der Integrations- und Repräsentationsfunktion beizumessen; das Wahlergebnis spiegelt in der Regel die Willensartikulation der Wähler wider. Der Grad der Identifikation und der Interessensvertretung zwischen Wähler und Regierenden bzw. Mandatsträgern steht in direktem Zusammenhang mit der Wahlbeteiligung. Mangelnde Politikidentifizierung kann zu einer niedrigen Wahlbeteiligung führen; dies vermag sich wiederum auf die Legitimität einer Regierung auswirken.

> „Für die Lebendigkeit der Demokratie ist es von entscheidender Bedeutung, in welchem Maße die Bürgerinnen und Bürger von ihren in der Verfassung garantierten Rechten Gebrauch machen und damit Einfluss auf die politische Willensbildung nehmen. Die Ausübung des Wahlrechts, mit der über die Zusammensetzung der demokratischen Vertretungen in Gemeinde, Land und Bund entschieden wird, spielt dabei die zentrale Rolle“ [Statistisches Bundesamt 2004, 168].

Das dargestellte liberale Konzept von Demokratie lässt also eine herrschende Gruppe zu, die ihren Legitimationsanspruch aus kompetitiven Wahlen zieht. Gleichzeitig wird versucht, diese Gruppe durch das Prinzip der Gewaltenteilung, die Wahrung der Menschenrechte, das Recht auf Opposition und die Chance für die Wähler, selbst in Gruppe der Herrschenden zu gelangen, zu kontrollieren. Wahlen kommt diesbezüglich eine sehr hohe Bedeutung zu, da sie für den Großteil der Bevölkerung die einzige direkte Partizipationsmöglichkeit darstellen. Neben der Mitgliedschaft in einer Partei, Gewerkschaft oder Bürgerinitiative sowie der Teilnahme an Demonstrationen bieten Wahlen und Plebiszite (also Volksbegehren, Volksentscheid, Volksabstimmung) eine Chance, in den politischen Prozess direkt einzugreifen. Der Anteil der Bevölkerung, der Mitglied in

einer politischen Partei ist, ist in Deutschland jedoch sehr gering. Nach Auswertung der ALLBUS-Daten[6] sind es 4, 2% der westdeutschen und 2, 1% der ostdeutschen Bevölkerung [vgl. Simonson 2003, 5]. Legt man die Mitgliederstatistiken der Parteien zugrunde, ist der Anteil noch geringer, nämlich bundesweit 1, 6 Mio. Bürger bzw. 2, 6% der Bevölkerung im wahlberechtigten Alter [vgl. Statistisches Bundesamt 2004, 177]. Hinzu kommt, dass unter den Parteimitgliedern Männer wesentlich stärker vertreten sind als Frauen. Beispielsweise liegt der Anteil der Frauen unter den Mitgliedern der SPD bei 29, 7%, unter den Mitgliedern der CDU sind 25, 1% Frauen [vgl. Statistisches Bundesamt 2004, 177f.]. Außerdem spielen Faktoren wie Bildung und Prosperität eine Rolle[7]. Faktisch ist die Wahl somit nur *eine* Partizipationsmöglichkeit im politischen Prozess eines liberal-demokratischen Systems, jedoch für die Masse der Bevölkerung auch *die einzige*.

1.1.2 Grundsätze von Wahlen und Abstimmungen nach dem Grundgesetz

1.1.2.1 Wahlen

Die erläuterten Bedeutungen und Funktionen finden ihre Grundlage in der deutschen Verfassung. „Alle Staatsgewalt geht vom Volke aus“ [Artikel 20 Absatz 2 Satz 1 GG]. Die Verankerung des Grundsatzes der Volkssouveränität im GG gewährleistet, dass der Ursprung aller Staatsgewalt beim Volk liegt. Das Prinzip der Volkssouveränität ist daher elementarer Grundsatz der deutschen Demokratie. Allerdings präzisiert Artikel 20 Absatz 2 Satz 2 GG, dass die Staatsgewalt „vom Volke in Wahlen und Abstimmungen und durch besondere Organe der Gesetzgebung, der vollziehenden Gewalt und der Rechtsprechung ausgeübt“ wird. Die Ausübung der Staatsgewalt durch Wahlen des Volkes und besonderer Organe verdeutlicht die repräsentative Ausgestaltung des demokratischen Systems durch das GG [vgl. Birkenmaier 2004, 8]. Offengelassen wird im Artikel 20 GG jedoch, welche Organe durch das Volk mittels Wahlen zu besetzen sind. Die Nennung aller drei Staatsgewalten eröffnet die grundsätzliche Möglichkeit, verschiedene Organe durch Wahlen bestimmen zu lassen. Im GG findet sich nur eine Regelung, die die Besetzung eines Staatsorgans durch Wahlen bestimmt. Artikel 38 Satz 2

[6] Die „Allgemeine Bevölkerungsumfrage der Sozialwissenschaften“ (ALLBUS) wird vom Zentrum für Umfragen, Methoden und Analysen (Mannheim) und dem Zentralarchiv für empirische Sozialforschung (Köln) durchgeführt und erhebt seit 1980 alle zwei Jahre einen repräsentativen Querschnitt der Bevölkerung mit einem teils stetigen, teils variablen Fragenprogramm. Abrufbar unter http://www.gesis.org/Dauerbeobachtung/Allbus/index.htm (Verifizierungsdatum: 16.09.2005).
[7] Vgl. [Engels 2004].

GG überträgt die Wahl zum Bundestag klar dem Volk. Zusätzlich wird festgelegt, dass die Abgeordneten

> „in allgemeiner, unmittelbarer, freier, gleicher und geheimer Wahl von den wahlberechtigten Deutschen nach den Grundsätzen einer mit der Personenwahl verbundenen Verhältniswahl gewählt [werden]“ [§ 1 Absatz 1 Bundeswahlgesetz[8]].

Die Entscheidung für ein personalisiertes Verhältniswahlrecht ist somit im BWG festgelegt, nicht im Grundgesetz. Dort ist nur geregelt, wer wahlberechtigt ist[9] und unter welchen Bedingungen der deutsche Bundestag gewählt wird. Die in Artikel 38 Satz 1 GG definierten Wahlrechtsgrundsätze werden durch Artikel 28 Absatz 1 Satz 2 GG auch auf Länder-, Kreis- und Kommunenebene zum demokratischen Maßstab erklärt und erlangen dadurch allgemeine Gültigkeit bei allen innerdeutschen Wahlen.

Das allgemeine Wahlrecht besagt, dass alle deutschen Staatsbürger abstimmungsberechtigt sind, unabhängig von Konfession, Bildung, Geschlecht, Sprache, Einkommen, Beruf oder politischer Überzeugung [vgl. Schreiber 2002, 87f.]. Laut § 12 BWG bezieht sich das allgemeine Wahlrecht auf „alle Deutschen im Sinne des Artikels 116 Absatz 1 des GG“. Bedingungen sind die Volljährigkeit und die Wohnhaftigkeit in Deutschland, zudem darf die Person nach § 13 BWG nicht vom Wahlrecht ausgeschlossen sein. Sonderregelungen gelten für Beamte, Soldaten, Angestellte und Arbeiter im öffentlichen Dienst, die „auf Anordnung ihres Dienstherren außerhalb der Bundesrepublik Deutschland leben, sowie Angehörige ihres Hausstandes“ sowie für Seeleute, Binnenschiffer und im Freiheitsentzug befindliche Personen [§ 12 BWG].

Die Unmittelbarkeit der Wahl bedeutet die direkte Wahl der Abgeordneten, d.h. ohne Zwischenschaltung von Wahlmännern oder Delegierten, die nach eigenem Ermessen die Abgeordneten wählen [vgl. Schreiber 2002, 90]. Die Wählerstimmen werden vielmehr direkt für die Verteilung der Parlamentssitze verwertet.

Der Grundsatz der freien Wahl bezweckt die unbeeinflusste Stimmabgabe der Bürger. Weder von privater noch von öffentlicher Seite darf auf die Willensbildung oder die Wahlentscheidung Einfluss genommen werden. Während der Wahlzeit ist in, an und vor dem Wahlgebäude „jede Beeinflussung der Wähler durch Wort, Ton, Schrift oder Bild sowie jede Unterschriftensammlung verboten“ [§ 32 Absatz 1 BWG]. Ebenso ist die

[8] Das Bundeswahlgesetz wird im Folgenden als BWG bezeichnet.
[9] GG Artikel 38 Satz 2.

Veröffentlichung der Ergebnisse von Wahlbefragungen nach der Stimmabgabe über Inhalt der Wahlentscheidung vor Beendigung der Wahl untersagt[10]. Die nichtzulässige Beeinflussung der Willensbildung bzw. Willensäußerung betrifft nicht nur die inhaltliche Entscheidung der Stimmabgabe, sondern auch, ob überhaupt bzw. ungültig gewählt wird [vgl. Birkenmaier 2004, 58].

Das gleiche Wahlrecht beinhaltet einerseits, dass jeder Wahlberechtigte das für ein demokratisches System erforderliche aktive Wahlrecht in formal gleicher Weise ausüben kann [vgl. BVerfGE 16, 138] und jede Stimme den gleichen Zähl- und Erfolgswert besitzt [vgl. Birkenmaier 2004, 13]. Dies beinhaltet auch die Verhinderung der mehrfachen Stimmabgabe und die gleiche Wertung von Präsenz- und Briefwahl. Jede Art von Gewichtung der Stimmen ist also unrecht. Andererseits muss auch die Chancengleichheit der Parteien gewährleistet sein, also die Gleichheit des passiven Wahlrechts. Denn „wählbar ist, wer am Wahltage (1) Deutscher im Sinne des Artikels 116 Absatz 1 des GG ist und (2) das achtzehnte Lebensjahr vollendet hat“ [§ 15 Absatz 1 BWG]. Eine Benachteiligung demokratischer Parteien und Wahlbewerber durch die Wahlgesetzgebung ist unzulässig [vgl. Wild 2003, 177].

Die geheime Wahl regelt die Nichtnachprüfbarkeit der Wählerentscheidung. Es muss sichergestellt sein, dass die Stimmabgabe für Dritte nicht einsehbar ist und kein Zusammenhang zwischen abgegebenem Votum und Wähler hergestellt werden kann [vgl. Schreiber 2002, 141]. Die besondere Bedeutung der Geheimheit der Wahl verdeutlicht auch Artikel 21 der Allgemeinen Erklärung der Menschenrechte von 1948[11]. Dort heißt es, dass der Wille des Volkes „durch regelmäßige, unverfälschte, allgemeine und gleiche Wahlen mit *geheimer* Stimmabgabe oder einem gleichwertigen freien Wahlverfahren zum Ausdruck kommen“ muss. In § 33 Absatz 1 BWG wird zudem sicherstellt, dass zur Aufbewahrung der Stimmen nur Wahlurnen verwendet werden, die die Wahrung des Wahlgeheimnisses garantieren. Der Grundsatz der Geheimhaltung der Wahl steht in enger Beziehung zur Freiheit der Wahl. Denn nur die volle Gewährleistung der geheimen Wahl kann die uneingeschränkte Wahlfreiheit garantieren.

10 § 32 Absatz 2 BWG.
11 Resolution 217 A [III] der Generalversammlung vom 10. Dezember 1948.

Um die Zulässigkeit der Internetwahlen beurteilen zu können, werden die genannten Wahlrechtsgrundsätze im Späteren auf den Fall des E-Votings übertragen und geprüft[12].

1.1.2.2 Abstimmungen

Während es bei Wahlen um die Entscheidung der Bürger über die Zusammensetzung der Parlamente geht, betreffen Abstimmungen meist Sachentscheidungen. Mit der Verankerung von Abstimmungen in Artikel 20 Absatz 2 Satz 2 GG wird die Möglichkeit zur direkten und unmittelbaren Staatsgewalt festgelegt. Bei weiterer Betrachtung wird deutlich, dass diese Möglichkeiten auf Bundesebene eine selten vorgesehene Ausnahme darstellen [vgl. Birkenmaier 2004, 7]. In Artikel 29 GG werden Plebiszite zugelassen, jedoch nur, wenn es um die Veränderung von Ländergrenzen geht. „Maßnahmen zur Neugliederung des Bundesgebietes ergehen durch ein Bundesgesetz, das der Bestätigung durch Volksentscheid bedarf“ [Artikel 29 Absatz 2 GG]. Neben dem Volksentscheid wird noch der Fall des Volksbegehrens und der Volksbefragung geregelt. So können Einwohner bestimmter Gebiete die Neuregelung ihrer Landeszugehörigkeit durch Volksbegehren erreichen[13], außerdem ist die Zustimmung der durch eine gesetzlich vorgeschlagene Neugliederung betroffenen Bürger durch Volksbefragung festzustellen[14].

Die plebiszitären Elemente sind somit hauptsächlich unmittelbar-demokratische Mitwirkungsmöglichkeiten auf kommunaler Ebene. Ob, in welcher Form und unter welchen Vorraussetzungen unmittelbare Volksbeteiligung in den Bundesländern verankert ist, bestimmen die jeweiligen Länderverfassungen in Ausführungsgesetzen und Abstimmungsordnungen [vgl. Weixner 2002, 101]. Neben verfassungsrechtlichen Normen, die die einfache Landesgesetzgebung betreffen, bestehen Regelungen zur Änderung der Landesverfassung, die entweder ausdrücklich untersagt[15], notwendige Bedingung[16] oder unter bestimmten Bedingungen möglich sind. In einigen Verfassungen finden sich auch Grundlagen für plebiszitäre Personalentscheidungen wie die Auflösung des Parlaments oder die Abberufung der Regierung. Zusätzlich bestehen sogenannte Negativkataloge, die Sachfragen enthalten, über die keine Volksentscheide, Volksbegehren oder Volksbefragungen stattfinden dürfen. Eine genauere Untersuchung der einzelnen Verfahren und

[12] Zu den demokratietheoretischen Anforderungen vgl. Kapitel 2.3.
[13] Artikel 29 Absatz 4 GG.
[14] Artikel 29 Absatz 5 GG.
[15] Berlin und Saarland.
[16] Hessen und Bayern.

Möglichkeiten ist an dieser Stelle nicht geboten, dennoch können diese plebiszitären Elemente

> „zur Intensivierung und Vervielfältigung von Demokratie auf der kommunalen Ebene [führen], indem die Beteiligungsmöglichkeiten der Selbstverwaltung gerade zur Kompensation des Fehlens echter Mitwirkungsmöglichkeiten auf den vorgelagerten Staatsebenen dienen können" [Schliesky 1999, 93].

1.2 Das Internet in der Demokratie

Neben ihren institutionellen Voraussetzungen stellt sich Demokratie auch als ein stetiger Kommunikationsprozess zwischen Regierenden und Regierten dar. Die Zielsetzung sollte die Beteiligung aller von einer Entscheidung Betroffenen an der Entscheidungsfindung sein [vgl. Ewert et al. 2003, 229]. Eine Voraussetzung für das Funktionieren einer derartigen Demokratie ist in modernen Gesellschaften wie der Bundesrepublik Deutschland eine mediale Infrastruktur. Mit der Verbreitung des Internets bieten sich Möglichkeiten, diese Infrastruktur für neue Wege der Information, Kommunikation und Partizipation zu nutzen.

Das Internet ist das am schnellsten wachsende Medium aller Zeiten. Während im Jahr 1997 6, 5% der Deutschen ab 14 Jahren mindestens gelegentlich das Internet nutzten, sind es im Jahr 2004 bereits 55, 3% [vgl. Eimeren et al. 2004, 351]. Dieses steigende Nutzerpotential beeinflusst die Einsatzmöglichkeiten des Internets deutlich. Nach dem elektronischen Handel (E-Commerce) stellt auch der öffentliche Sektor seine Dienstleistungen auf Bundes-, Länder- und Kommunalebene teilweise online zur Verfügung. Angesichts der weitreichenden Bemühungen in In- und Ausland, das Internet in der öffentlichen Verwaltung zu nutzen, ist von einer umfassenden Reorganisation von Verwaltungsvorgängen mittels internetgestützter Anwendungen zu sprechen[17].

1.2.1 E-Government und E-Demokratie: eine Definition

Der Begriff des Electronic Government (E-Government) ist in der Literatur nicht einheitlich definiert[18]. Laut des Bundesinnenministeriums umfasst er

[17] Vgl. z.B. die Studie ‚E-Europe' zum elektronischen Serviceangebot der Öffentlichen Hand, die Cap Gemini Ernst & Young im Auftrag der Europäischen Kommission durchgeführt hat; abrufbar unter http://www.de.capgemini.com/servlet/PB/show/1566999/Capgemini_eEurope_2005.pdf (Verifizierungsdatum: 16.09.2005).
[18] Vgl. z.B. [Jansen/Priddat 2001], [Hill 2002], [Birkenmaier 2004], [Winkel 2004].

> „alle Prozesse der öffentlichen Willensbildung, der Entscheidungsfindung und Leistungserstellung in Politik, Staat und Verwaltung, soweit diese unter weittestgehender Nutzung von Informations- und Kommunikationstechnologien stattfinden“[19].

Somit wird vom E-Government mehr erwartet als eine reine Online-Präsentation der Behörden oder die schlichte Bereitstellung von Formularen als Download. Es geht vielmehr um einen Ausgleich zwischen Verwaltungseffizienz einerseits und Stärkung der bürgerlichen Partizipation andererseits [vgl. Bertelsmann Stiftung 2001, 3]. Im Leitfaden für Behördenleiter des Bundesamtes für Sicherheit in der Informationstechnik bezeichnet E-Government die Nutzung des Internets und anderer elektronischer Medien zur Einbindung der Bürger und Unternehmen in das Verwaltungshandeln sowie zur verwaltungsinternen Zusammenarbeit. Einerseits impliziert das ‚elektronische Regieren' also die elektronischen Bürgerdienste und Informationsangebote (E-Administration), andererseits geht es um die Einbindung partizipativer Elemente für die Bürger (E-Demokratie) [vgl. Bertelsmann Stiftung 2001, 4].

Der administrative Teil beinhaltet die

> „IT- gestützte Abwicklung von Prozessen an der Schnittstelle von Verwaltung und Verwaltungsklientel (Bürger, Unternehmen) [sowie] an der Schnittstelle von Verwaltung und ihren Geschäftspartnern (etwa im Ausschreibungs- und Beschaffungswesen)“ [Winkel 2004, 8].

Die digital vermittelten Dienstleistungen stehen hierbei im Vordergrund, der Bürger wird als Dienstleistungsnehmer oder Kunde verstanden, der Verwaltungsverfahren online in Anspruch nimmt [vgl. Bieber 2002, 180].

Der Bereich der elektronischen Demokratie soll die Mitwirkung der Bürger an der

> „politischen Willensbildung, welche idealtypisch in die Stufen der Aufnahme von Informationen, des Diskurses zum Abgleich von Problemen, Wahrnehmungen und Interessen sowie der Vollendung des Willensbildungsprozesses durch die politische Entscheidung unterteilt werden kann“ [Winkel 2004, 8]

fördern. E-Demokratie schließt dabei die politische Willensbildung durch Online-Information ebenso ein wie die politische Partizipation, die von staatlicher Seite angeboten wird und auch aus der Zivilgesellschaft heraus entstehen kann.

Hierauf aufbauend wird der Begriff des E-Government im Folgenden als Summe der E-Administration und der E-Demokratie gesehen, wobei E-Voting als partizipatives Ele-

[19] Vgl. http://www.bmi.bund.de/cln_028/nn_121572/Internet/Navigation/DE/Service/Lexikon/GenericDynCatalog,lv2=121688,lv3=132658.html (Verifizierungsdatum: 16.09.2005).

ment Letzterer zuzuordnen ist. Alle Anwendungen der E-Administration und der E-Demokratie können auf unterschiedlichen Ebenen realisiert werden: der Informations-, der Kommunikations- sowie der Transaktionsebene. Die Ebene der digitalen Informationsbereitstellung beinhaltet keinerlei interaktive Funktion, sondern einen reinen Informationsservice. Als netzbasierte Kommunikation ist ein direkter Austausch mit Rückkopplung möglich, d.h. es handelt sich um computervermittelte Kommunikation. Auf der Ebene der Transaktion werden Abläufe ohne Medienbruch rechtsverbindlich abgewickelt, so etwa die vollständige Online-Abwicklung eines Antrags oder der Steuererklärung [vgl. Winkel 2004, 8]. Trotz der im September 2000 gestarteten Initiative der Regierung ‚Bund Online 2005'[20], die alle onlinefähigen Dienstleistungen der Bundesverwaltung bis Ende 2005 elektronisch zur Verfügung stellen will, sind Anwendungen ohne Medienbruch bis heute eine seltene Ausnahme.

1.2.2 Funktionen des Internets für die Demokratie

1.2.2.1 Informationsfunktion

Als eine der wichtigsten Voraussetzungen der freiheitlichen Demokratie ist die Informationsfreiheit in Artikel 5 Absatz 1 Satz 1 GG verankert. Öffentlichkeit, Bürger und Massenmedien sollen die Möglichkeit zu einer fundierten Meinung aufgrund objektiver Tatsachen haben.

> „Information ist die Grundvoraussetzung für Bürgerinnen und Bürger, um mitreden und sich engagiert in den politischen Willensbildungsprozessen beteiligen zu können" [Schily 2001,1].

Unabhängig von der Frage, ob die ‚traditionellen' Informationsmöglichkeiten diesen Anspruch erfüllen, steigen die Möglichkeiten der Bürger zur Information durch das Internet. Sowohl der öffentliche Sektor als auch Parteien und Verbände unternehmen auf Bundes-, Länder- sowie Kommunalebene Anstrengungen, neue Wege zur Informationsbereitstellung zu nutzen [vgl. Welz 2002, 6f.]. Indem die Informationen auf einem öffentlich zugänglichen Server bereitgestellt werden, sinken die Bereitstellungskosten und die Information kann direkt und ohne Vermittler weitergegeben werden. Durch die Verknüpfung von Ton, Bild und Text entsteht eine multimediale Vielseitigkeit. Informationen können umfassender aufbereitet und mit Hintergrundinformationen über Verlinkungen in einen Kontext gesetzt werden. Diese Verknüpfung kann ein ganzheitliches Verständnis und eine fundiertere Meinungsbildung fördern [vgl. Birkenmaier 2004,

[20] Siehe auch www.bundonline2005.de (Verifizierungsdatum: 16.09.2005).

253]. Als weitere Vorteile sind die ständige Verfügbarkeit unabhängig von Zeit und Ort, die Aktualisierbarkeit der Information und nahezu unbegrenzte Kapazitäten zu nennen.

> „Das Internet bietet mit seiner kommunikationstechnischen Infrastruktur die nie zuvor gekannte Möglichkeit, schnell, günstig und mit geringem Aufwand an Informationen aus nahezu allen Teilen der Welt zu gelangen“ [Hoecker 2002, 37].

Bereitgestellt werden sowohl unverbindliche Informationen, z.B. die sogenannten Stadtinformationssysteme, die über aktuelle Geschehnisse bis hin zu Behördengängen informieren [vgl. Korff 1999, 197], als auch verbindliche Informationen, für die besondere Anforderungen gelten.

Verkündigung und Bekanntmachung von Normen und Beschlüssen, wie z.B. Rechtsverordnungen der Parlamente, erfolgen im Regelfall auf Länderebene im Landesgesetzblatt. Artikel 82 Absatz 1 GG bestimmt die Verkündigung der Bundesgesetze und Rechtsverordnungen des Bundes im Bundesgesetzblatt. Sowohl auf Bundesebene als auch in einigen Bundesländern gibt es mittlerweile Rechtssammlungen, die Rechtsvorschriften online stellen[21], jedoch

> „steht die Veröffentlichung in einer solchen Rechtssammlung der Bekanntgabe in einem herkömmlichen Veröffentlichungsblatt nie gleich. Sie ist immer nur als zusätzliche Bekanntgabemöglichkeit zu betrachten“ [Birkenmaier 2004, 145].

Die Verkündung in Bundes- oder Landesgesetzblatt soll sicherstellen, dass den vom Gesetz potentiell Betroffenen die Möglichkeit gegeben wird, sich über den Inhalt zu informieren. Die alleinige Veröffentlichung im Internet genügt bei der momentanen Verbreitung des Internets dieser Anforderung nicht.

Der potentielle Zugang zu Informationen kann die Transparenz fördern und damit auch die Verständlichkeit des öffentlichen Sektors gegenüber den Bürgern. Dies gilt besonders für den parlamentarischen Bereich, in dem das Internet zur Veröffentlichung und Erklärung politischer Entscheidungsprozesse genutzt werden kann. Eine verständliche Darstellung der parlamentarischen Debatten fördert die Transparenz der Legislative, indem

> „bisher nicht-öffentliche oder halb-öffentliche parlamentarische Diskussions- und Abstimmungsprozesse einer medialen Öffentlichkeit verstärkt zugänglich gemacht werden“ [Birkenmaier 2004, 254].

[21] Siehe auch die Bundesrechtsammlung unter www.bmj.bund.de (Verifizierungsdatum: 16.09.2005).

Auf nationaler wie auf internationaler Ebene[22] wird zudem verstärkt das Recht der Bürger auf Zugang zu prinzipiell allen Informationen des öffentlichen Sektors diskutiert. Die sogenannten Informationsfreiheitsgesetze (IFG) haben einzelne Bundesländer bereits verabschiedet[23]; das Informationsrecht erstreckt sich auf die Unterlagen der Landesbehörden genauso wie auf die Akten der Kreisverwaltungen oder der Gemeinden. Auf Bundesebene ist der Gesetzentwurf eingereicht[24]. Das Gesetz wird 2006 in Kraft treten [vgl. Krempl 2005]. In dem Entwurf wird das Internet explizit als „allgemein zugängliche Quelle" bezeichnet [Müntefering 2004, zu § 9 Absatz 3, 16]. Außerdem sollen die Behörden „Pläne und Verzeichnisse sowie weitere geeignete Informationen in elektronischer Form allgemein zugänglich machen" [ebd. § 11 Absatz 3].

Das Internet kann also die Informationsmöglichkeiten für Bürger bezogen auf Aktualität und allgemeine Verfügbarkeit erheblich erhöhen. Aufgrund der Verbreitungs- und Nutzerzahlen[25] ist das Internet bislang - und sicherlich auch in naher Zukunft - jedoch nur als ergänzender Service, nicht aber als alleiniges Medium zu nutzen, da andernfalls den grundgesetzlichen Anforderungen an die Publizität des Rechts nicht genügt wird. Ein weiterer Nachteil des Internets ist die prinzipielle Offenheit, die quasi jedem die Chance bietet, Informationen zu verbreiten. So kann die Qualität zugunsten der Quantität von Information sinken. Bei der stetigen Zunahme von Information ist es gerade für den Laien schwierig, wichtige von unwichtiger bzw. richtige von falscher oder schlecht recherchierter Information zu unterscheiden. Insbesondere das Differenzieren von politischer und sachlicher Information und Agitation bezogen auf die Relevanz der Quellen erfordert nicht nur Medienkompetenz[26], sondern auch Vorerfahrungen und Wissen sowie in anderen Kontexten erworbene Fähigkeiten [vgl. Hoecker 2002, 39].

Die Möglichkeit der permanenten Informationsveröffentlichung wirkt sich einerseits also auf die Quantität der Information aus, andererseits auch auf die ‚Halbwertszeit der Information', die sich im Internet rapide verringert, da Information schneller aktualisiert werden kann als in den klassischen Medien. Große Mengen an alten und an vermeint-

[22] Vgl. z.B. www.informationsfreiheit.info/de/ (Verifizierungsdatum: 16.09.2005).
[23] IFGs sind z.B. in Schleswig-Holstein, Brandenburg, Berlin und Nordrhein-Westfalen in Kraft. Vgl. dazu [Schoch 2002, 149].
[24] Drucksache 15/4493 vom 14.12.2004.
[25] Vgl. Kapitel 1.2 sowie ausführlich Kapitel 5.1.1.
[26] Medienkompetenz steht im Folgenden für die Kenntnis und den sicheren Umgang mit Computer und Internet.

lich aktuelleren, neu hinzugefügten Daten erschweren die Filterung der relevanten Informationen. Zusätzlich ist zu bedenken,

> „dass Eigenangebote politischer Akteure immer im ‚PR-Geruch' stehen, so dass die Glaubwürdigkeit der Mitteilungen nicht sehr hoch ist" [Donges & Jarren 1999, 97].

Neben Zweifeln an der Qualität der Internetinformation stellt sich die Frage nach der Bereitschaft der Bürger, diese Information auch zu nutzen. Zwar ist das Nutzungsmotiv „zielgerichtet bestimmte Angebote suchen" auf Platz zwei der sechzehn stärksten Nutzungsmotive [vgl. Eimeren et al. 2004, 356], jedoch geben nur 20% der Befragten an, politische Informationsangebote zu nutzen [vgl. ebd., 363]. Die verbesserten Informationsmöglichkeiten sagen somit noch nichts über eine bessere Informiertheit der Bürger aus. Es

> „stellt sich grundsätzlich die Frage, warum Bürgerinnen und Bürger im digitalen Zeitalter auf einmal ein ausgeprägtes politisches Interesse entwickeln und zu gut informierten und bis ins Detail kenntnisreichen Wählern/Wählerinnen werden sollten" [Hoecker 2002, 39].

Es besteht also durchaus Skepsis, dass aufgrund wachsender Informationstechnik auch das Bedürfnis nach mehr und detaillierterer Information aus dem politischen Bereich wächst [vgl. Kleinsteuber 1999, 52ff.]. Dass das Internet dieses Bedürfnis fördert, ist wissenschaftlich nicht belegt [vgl. Birkenmaier 2004, 259]. Aufgrund der wachsenden Informationsangebote im Internet können Bürger einen fundierteren Willensbildungsprozess vollziehen und ihre politische Entscheidung qualifizierter treffen, doch ob das Internet zu einer umfassenden politischen Informiertheit in breiten Teilen der Bevölkerung führen kann, ist fraglich.

1.2.2.2 Kommunikations- und Partizipationsfunktion

Der politische Willensbildungsprozess erfordert neben der reinen Information über Entscheidungen und Prozesse auch Prozeduren, in denen sich der Wille bilden kann. Möglich ist dies in zweierlei Formen: durch interpersonale Kommunikation und durch Massenkommunikation [vgl. Niedermayer 2001, 133]. Beide Kommunikationswege tragen

> „für das Individuum jeweils durch Information zu Wissenserwerb und durch Interpretation zur Meinungsbildung und damit [...] zur Reduktion von Unsicherheit über eine komplexe, nicht unmittelbar erfahrbare politische Umwelt bei" [Schabedoth et al. 1995, 239].

Der Prozess der Willensbildung wird traditionell durch Parteien und Massenmedien beeinflusst, die eine Grundlage für eine gesellschaftliche Diskussion bieten [vgl. Meyer

2001, 20]. Im Idealfall bauen Bürger einen hohen Wissensstand über Probleme und mögliche Lösungen, die verschiedene politische Lager anbieten, auf und können so ihren Willen in die Politik einbringen, z.B. in Form von Initiativen, Demonstrationen und vor allem durch Wahlen.

> „Insofern sind in der Demokratie nicht nur formale Möglichkeiten der Beteiligung der Bürger von Bedeutung, sondern auch Beteiligungsmöglichkeiten an der sich im täglichen politischen Prozess konkretisierenden öffentlichen Meinung relevant“ [Birkenmaier 2004, 261].

Das Internet bringt in diesem Sinne neue Wege der Kommunikation mit sich. Aufgrund seiner Interaktivität bietet das Internet Möglichkeiten zur direkten Kommunikation. Die hierarchische ‚One-to-many’-Kommunikation der traditionellen Medien kann in die Form einer horizontalen ‚Many-to-many’-Kommunikation überführt werden [vgl. Meyer 2001, 177]. So können sich Bürger in Chats, Foren oder per Email mit ihren Anliegen und Meinungen direkt an Verwaltungen, Parteien, Parlamente oder einzelne Abgeordnete wenden. Letztlich besteht auch die Möglichkeit zur Umkehrung in eine ‚Many-to-one’-Kommunikation.

Gleichfalls kann das Internet als Instrument der Organisation örtlicher und überörtlicher Handlungsnetze in der Zivilgesellschaft fungieren[27]. Gerade lokale und kommunale Angelegenheiten finden unter Bürgern große Resonanz. Deshalb sind in fast allen Internetauftritten deutscher Großstädte Möglichkeiten zur Bürgerbeteiligung, hauptsächlich im Rahmen der baulichen Stadtentwicklung und des Flächennutzungsplans, vorhanden [vgl. Initiative eParticipation 2004, 18]. Aber auch in der Legislative bietet das Internet Möglichkeiten zu mehr Partizipation der Bürger. Auf Länder- und Bundesebene ist die Bereitstellung von Gesetzesentwürfen zu organisierten Diskussionszwecken denkbar. Auf die nötigen Hintergrundinformationen kann kontextbezogen verlinkt werden, so dass eine qualifizierte Meinungsbildung möglich ist und der Bürger mit externem Sachverstand neue Argumente einbringen könnte. Auf diese Weise wird nicht nur die Transparenz des Gesetzgebungsprozesses gefördert, sondern auch die Akzeptanz der mitgestalteten Gesetze und Verordnungen seitens der Bürger [vgl. Leggewie 1998, 28]. Vorstellbar wäre auch ein unverbindliches Abstimmungsverfahren von staatlicher Seite, bei dem auf Internetseiten eine Befragung zu einem bestimmten Thema im Sinne von ‚da-

[27] Vgl. [Bieber & Hebecker 1998].

für' bzw. ‚dagegen' der Meinungsäußerung dienen kann[28]. Problematisch bei diesen Partizipationsverfahren ist jedoch die Frage, inwiefern die Bürgerbeteiligung in derartigen unverbindlichen Diskussionen und Abstimmungen tatsächlich beachtet wird. So können diese Beteiligungsmöglichkeiten auch eine unerwünschte Wirkung haben, zumal es zweifelhaft ist, dass es nur *eine*, einheitliche bürgerliche Meinung gibt. Die Nichtbeachtung der bürgerlichen Meinung kann „Unverständnis gegenüber dem Verhalten der Repräsentanten hervorrufen, und destabilisierend auf das politische System wirken" [Birkenmaier 2004, 262]. Es müsste also eine Feedbackfunktion bedacht werden, die den Bürger darüber aufklärt, wer seine Anregungen wie erhält bzw. verarbeitet und warum sie eventuell nicht entsprechend umgesetzt werden.

Neben den genannten staatlichen Angeboten gibt es zahlreiche Angebote diverser gesellschaftlicher Gruppen, z.B. auf den Internetseiten von Parteien, herkömmlichen Massenmedien und Interessensgruppen [vgl. Leggewie 1998, 34]. Bei entsprechendem Interesse der Massenmedien können solche ‚Single-Issue-Gemeinschaften', also Gemeinschaften, die sich nur zu einem speziellen Thema formieren, ihr Anliegen in den staatlichen Willensbildungsprozess einbringen und eventuell eine Anschlusskommunikation in den staatlichen Institutionen provozieren [vgl. Marschall 1998, 52].

Wie bei der reinen Informationsfunktion stellt sich auch bei der Kommunikations- und Partizipationsfunktion die Frage, ob ein vermehrtes Angebot das bürgerliche Interesse an mehr Partizipation fördert und die Beteiligungschancen tatsächlich genutzt werden, denn „der Weg vom schlichten Informationsangebot bis zur bürgerschaftlichen Aktivität [ist] lang" [Kamps 2001, 31]. Da schon das reine Informationsangebot keine Schlüsse auf ein gesteigertes Interesse an politischer Information zulässt, ist eine Steigerung der Partizipationsbereitschaft erst recht schwer vorstellbar. Allerdings bezieht sich in Deutschland die Debatte über den Einsatz des Internets im öffentlichen Sektor hauptsächlich immer noch auf reine E-Government-Projekte im Sinne von Verwaltungsverfahren [vgl. Initiative eParticipation 2004, 4]. Mit vermehrtem Angebot kann möglicherweise das Interesse steigen, zumal das politische Interesse in engem Zusammenhang zur eigenen Betroffenheit steht [vgl. Roth 1997, 404 ff.]. Insofern stellt sich die

[28] So initiierte die griechische EU-Präsidentschaft das Experiment ‚E-Vote', in der unverbindlich darüber abgestimmt wurde, ob z.B. die Bürger direkt über die europäische Verfassung abstimmen sollten. Vgl. dazu [Lührs 2004].

Frage nach der Auswahl der Verfahren, an denen die Bürger direkt beteiligt werden sollen, wie also der Grad des allgemeinen Interesses bestimmt wird.

Des Weiteren ist zu beachten, dass politische Willensbildung mit Öffentlichkeit verknüpft, die Öffentlichkeit des Internets aber virtuell ist. Zwar sind Online-Chats und Foren ebenso wie Interaktionsangebote auf staatlichen Internetseiten in der Regel öffentlich zugänglich, somit scheint das Internet den Idealen einer demokratischen Öffentlichkeit zu genügen. Bei dieser ‚virtuellen Öffentlichkeit' haben jedoch nicht alle Bürger Zugang. Kritiker sehen in der Virtualisierung der Politik zusätzlich eine Gefahr für das politische System. Denn gerade die Öffentlichkeit ist ein Faktor der Kontrolle des staatlichen Handelns [vgl. Zippelius 2003, 192]. So sind nach Artikel 42 Absatz 1 Satz 1 GG die Verhandlungen des Bundestages öffentlich, darüber hinaus finden z.B. Wahlen und die Stimmauszählung in einem öffentlichen Raum statt. Da nicht jeder Bürger de facto über die gleichen Zugangsmöglichkeiten zur ‚virtuellen Öffentlichkeit' verfügt, sollten die neuen Wege bei allem Potential die herkömmlichen Verfahrensweisen nicht ersetzen. Als Ergänzung erweitert das Internet das Angebot zur Kommunikation und Partizipation für die Bürger.

Trotz dieser Bedenken stehen mit den neuen Kommunikationswegen auch Mittel zur Verfügung, den jeweiligen Repräsentanten die Meinungen und Einstellungen der Bürger näher zu bringen. Die Interaktivität des Internets ermöglicht eine asynchrone Kommunikation. Der traditionelle Kommunikationsweg über die Massenmedien kann umgangen werden, zudem vermittelt

> „die direkte Kommunikation zwischen Abgeordneten und Bürgern [..] die tatsächlichen Interessen der Bevölkerung und nicht die derjenigen Minderheiten, die exklusiven Zugang zu den Massenmedien besitzen" [vgl. Birkenmaier 2004, 273].

Es erscheint dennoch wahrscheinlich, dass diese Kommunikationsmöglichkeiten eher von bislang ohnehin politisch Engagierten genutzt werden. Die Annahme, dass infolge der Internetnutzung die Meinung jedes Bürgers Gewicht bekommt, erscheint fraglich. Der steigende Emailversand erschwert (besonders durch sogenannte Spam-Mails[29]) die persönliche und qualifizierte Beantwortung ernstgemeinter Zuschriften, so dass die vereinfachte Kommunikation zugleich zu einer Kommunikationsüberflutung führen kann. Die Rückkopplungsmöglichkeiten drohen unter der Fülle der Kommunikation zu ersti-

[29] Spam-Mails sind Emails, die unangefordert an eine große Anzahl von Empfängern verschickt werden, meist zu Werbezwecken.

cken [vgl. Clemens 1998, 152f.]. Die individuelle Email-Kommunikation vermittelt nur ein allgemeines Meinungsbild der Bevölkerung. Grundsätzlich bietet die Kommunikations- und Partizipationsfunktion des Internets dennoch Potential zur verbesserten Wahrnehmung des Volkswillens.

2 Anforderungen an Internet-Wahlen

Neben den Möglichkeiten der Information, Kommunikation und Partizipation in der Demokratie wird seit längerem über den Einsatz des Internets bei der technischen Durchführung einer politischen rechtsverbindlichen Entscheidung debattiert[30]. Da der Legitimitätsanspruch der Gewählten in liberal-demokratischen Staaten auf rechtmäßigen Wahlen beruht, sind trotz der technischen Änderung, die ein Online-Wahlsystem mit sich bringt, die genannten Wahlrechtsgrundsätze zu wahren.

Im Folgenden werden zunächst einige in der Literatur von Kritikern und Befürwortern diskutierte Erwartungen an das E-Voting vorgestellt, um danach verschiedene Typologien zu erstellen. Die demokratietheoretischen und sicherheitstechnischen Anforderungen an ein E-Voting-System werden anhand dieser Typologien erörtert; abschließend wird, aufbauend auf diesen Anforderungen, der mögliche technische Ablauf eines E-Voting-Systems skizziert.

2.1 Bislang diskutierte Erwartungen an das E-Voting

Eine Hoffnung, die mit Online-Wahlen verbunden wird, ist die der Rationalisierung des Wahlprozesses bezüglich der Kosten sowie des zeitlichen Ablaufs [vgl. z.B. Birkenmaier 2004, 50; Kubicek & Wind 2002, 102]. Bei herkömmlichen Wahlen betreffen die finanziellen Aspekte den Druck von Stimmzetteln, das Verschicken von Briefwahlunterlagen, die Ausstattung der Wahlräume sowie die Ernennung und Bezahlung von Wahlausschüssen, -beisitzern und –helfern. Abgesehen von Anschaffungs- und Implementierungskosten könnten sich zumindest langfristig die Wahlausgaben reduzieren und ein Mehrwert im Sinne von Einsparungen erreicht werden [vgl. Will 2002, 19].

Der Auszählungsprozess, der, insbesondere bei Landtags- und Kommunalwahlen, bei denen das Kumulieren und Panaschieren von Stimmen erlaubt ist, gestaltet sich meist langwierig. Bei technikgestützten Wahlen ist ein schnelles Auszählen der Stimmen denkbar. Gerade bei den genannten Landeswahlsystemen hätte die Rationalisierung des Wahlprozesses noch einen weiteren Vorteil bezüglich der Vereinfachung des Wahlsystems. Ein Rechenfehler des Wählers kann zur völligen Ungültigkeit seiner Stimmen

[30] Siehe z.B. das Forschungsprojekt ‚Wählen in elektronischen Netzwerken' (W.I.E.N.) als Zusammenschluss des Bundesministeriums für Wirtschaft und Arbeit, der Universität Osnabrück, des Landesbetriebs für Datenverarbeitung und Statistik (LDS) Brandenburg und T-Systems unter http://www.forschungsprojekt-wien.de/ (Verifizierungsdatum: 16.09.2005).

führen. Ein E-Voting-System könnte hier die Abgabe von unbewusst ungültig abgegebenen Stimmen verhindern [vgl. Buchstein 2002, 30].

In der Diskussion um zunehmende ‚Politikverdrossenheit' und zurückgehende Wahlbeteiligung wird die Internet-Wahl als Antwort gesehen, die den Legitimationsanspruch des demokratischen Systems verbessert. Gerade wahlberechtigte technik-affine Jugendliche, bei denen die Wahlbeteiligung bei der Bundestagswahl 2002 rund 10% unter dem Durchschnitt lag [vgl. Der Bundeswahlleiter 2003, 3], und Bürger, denen der bisherige Aufwand der Wahl größer erscheint als der Nutzen [vgl. Philippsen 2002, 139], könnten durch die ‚bequeme' Lösung der Internetwahl als aktive Wähler gewonnen werden. Auch die Gruppe der Wahlberechtigten, die am Wahltag kurzfristig durch Krankheit, Abwesenheit o.ä. verhindert ist und somit keine Briefwahl beantragen kann, würde von einem E-Voting-System profitieren, vorausgesetzt es ist keine vorherige Antragsstellung erforderlich. Doch selbst gegenüber der regulären Briefwahl hätte eine Wahl im Internet Vorteile, da hierbei keine ‚Voraus-Wahl' [Birkenmaier 2004, 54] aufgrund des Beförderungszeitraums des Wahlbriefes nötig wäre. Laut § 36 Absatz 1 BWG muss „der Wahlbrief spätestens am Wahltage bis 18.00 Uhr" beim Kreiswahlleiter eingehen, somit hat der Briefwähler nicht denselben Zeitrahmen zur Verfügung wie der Präsenzwähler.

Internetwahlen werden nicht zuletzt deshalb befürwortet, weil die Einführung eines funktionsfähigen Internetwahlsystems internationales Ansehen für die technische Offensive eines Landes mit sich brächte [vgl. z.B. Philippsen 2002, 140; Buchstein 2000a, 888].

Kritiker heben vor allem das Risiko der digitalen Spaltung hervor, die die Einhaltung der politischen Gleichheit gefährdet. Die erforderliche Medienkompetenz sowie der Zugang zum Internet trifft nicht alle wahlberechtigten Bürger in gleichem Maße. Gleichzeitig kann die technikbedingte gleiche Wertung der Stimmen durch bewusste Manipulation oder durch nicht korrekte Stimmzählung gefährdet sein und eine mehrfache Stimmabgabe ermöglichen [vgl. z.B. Will 2002, 18]. Ein E-Voting-System muss daher sowohl die Identifizierung des Wählers als auch Entkopplung des Votums von der Person des Wählers gewährleisten [vgl. z.B. Buchstein 2002, 51ff.]. Auch die Entwertung des Wahlvorgangs als symbolischer Akt gelebter Demokratie ist denkbar [vgl. z.B. Neymanns 2002b, 23ff.; Philippsen 2002, 141].

2.2 Eingrenzende Definitionen von E-Voting-Systemen

Der Begriff des E-Votings steht zunächst für eine Wahl, die, im Gegensatz zu klassischen Verfahren mit Stimmzettel und Urne, mithilfe eines elektronischen Gerätes durchgeführt wird. Es fallen also alle Wahlformen darunter, bei denen zwischen der Stimmabgabe und der Auszählung elektronische Geräte zum Einsatz kommen [vgl. Will 2002, 67]. Der Einsatz dieser elektronischen Wahlmaschinen ist ausdrücklich in § 35 BWG geregelt. Üblicherweise erfolgt die Abbildung des Stimmzettels auf einem Touchscreen. Die Stimmen werden im Wahlsystem elektronisch gespeichert[31].

Diese Begrifflichkeit ist für die vorliegende Arbeit zu weit gefasst. E-Voting wird vielmehr als eine Subkategorie der elektronischen Wahlform gesehen, bei der das Votum ausschließlich mithilfe des Internets übermittelt wird. Hierbei gilt es, grundsätzliche Kategorien zu bilden, die einerseits den Grad der örtlichen Dezentralisierung des Wahlvorgangs ausdrücken, andererseits den Status von E-Voting im Konzept der Stimmabgabe. Es lassen sich drei Kategorien unterscheiden, die den Grad der örtlichen Dezentralisierung des Wahlvorgangs beschreiben.

Bei einer Internetwahl im Wahllokal ist das Stimmgerät an das Internet angeschlossen und dabei wie die klassische Wahlurne in einer Wahlkabine im öffentlichen Wahlraum aufgestellt. Der Computer ist dabei bezüglich der installierten Komponenten kontrollierbar, das Stimmgerät vom Urnenserver räumlich und organisatorisch getrennt, d.h. das Votum wird an eine andere Stelle zum Auszählen übermittelt. Vorteil gegenüber der klassischen Wahl wäre eine schnellere Auszählung und die Aufhebung der Gebundenheit des Wählers an seinen Wahlkreis, d.h. der Wähler könnte von einem anderen Wahllokal aus für seinen Heimatwahlkreis abstimmen.

Eine andere Variante ist das sogenannte ‚Kiosk-Voting'. Hierbei wird das öffentliche und bezüglich der installierten Komponenten kontrollierbare Eingabegerät mit Internetzugang an öffentlich zugänglichen Räumen (z.B. in einer Bibliothek, im Bahnhof etc.) ohne die Anwesenheit von Wahlhelfern aufgestellt.

Die Internetwahl im individuellen Bereich schließlich erfolgt mittels eines beliebigen Computers mit Internetzugang. Denkbar wäre in dieser Kategorie auch die Stimmabga-

[31]Seit ihrer Einführung 1961 haben sich die Wahlmaschinen nicht flächendeckend durchgesetzt. Die möglichen Vorteile stehen wohl in keinem Verhältnis zu den relativ hohen Anschaffungs-, Transport-, Lager und Wartungskosten. In Köln kommen die Wahlmaschinen seit der Europawahl 1999 zum Einsatz. Siehe http://www.stadt-koeln.de/wahleninkoeln/wahlgeraete/index.html (Verifizierungsdatum: 16.09.2005).

be mit anderen internetfähigen Geräten wie einem Mobiltelefon oder einem Personal Digital Assistant (PDA) [vgl. Will 2002, 69].

Diese lokalen Unterschiede sind in zweifacher Hinsicht von zentraler Bedeutung. Zum einen wäre der Wahlrechtsgrundsatz der freien und geheimen Wahl mit zunehmender Dezentralisierung wahrscheinlich nicht voll zu gewährleisten [vgl. Buchstein 2002, 54], zum anderen spielt der sicherheitstechnische Aspekt, der durch die Entfernung verringerten Kontrollmöglichkeiten bezüglich der auf dem Computer befindlichen Software oder gegebenenfalls auch Malware[32], also bösartiger Software, eine Rolle.

Hinsichtlich des Status' des E-Votings im Konzept der Stimmabgabe besteht einerseits die Möglichkeit, die Stimmabgabe über das Internet als neue Regelform einzuführen, andererseits könnte sie als ergänzendes Angebot neben der Briefwahl oder als Ersatz dieser fungieren. Das folgende Schema veranschaulicht die unterschiedlichen Einsatzmöglichkeiten des E-Votings.

Status des E-Votings im Konzept der Stimmabgabe / Grad der örtlichen Dezentralisierung	Substituierung der herkömmlichen Urnenwahl	Ersatz der Briefwahl	Ergänzende Alternative neben Urnen- und Briefwahl
Wahllokal			
Wahlkiosk			
Individueller Bereich			

Abbildung 1: Typologien des E-Votings

2.3 Demokratietheoretische Anforderungen

2.3.1 Allgemeine Wahl

Nach der Auffassung des Bundesverfassungsgerichts[33] untersagt der Grundsatz der allgemeinen Wahl

> „den unberechtigten Ausschluss von Staatsbürgern von der Teilnahme an der Wahl überhaupt. Er verbietet dem Gesetzgeber, bestimmte Bevölkerungsgruppen aus politischen, wirtschaftlichen oder sozialen Gründen von der Ausübung des Wahlrechts auszuschließen" [BVerfGE 36, 139 (141); 58, 202 (205)].

[32] Zu den unterschiedlichen Typen von Malware vgl. Kapitel 2.4.2.2.
[33] Das Bundesverfassungsgericht wird im Folgenden als BVerfG bezeichnet.

Der Gesetzgeber ist deshalb bei der Einführung der Internetwahl dazu angehalten, die Benachteiligung von Bürgern ohne Internetzugang und/oder die erforderliche Medienkompetenz zu vermeiden. Zugleich gilt es, den technisch bedingten Ausschluss des Wählers, d.h. die Fehlleitung oder Veränderung des Votums aufgrund fremder Eingriffe zu verhindern und die Verfügbarkeit der Wahlstelle zu gewährleisten [vgl. Will 2002, 76]. Der drohende Ausschluss bzw. die Benachteiligung bestimmter Bevölkerungsgruppen, die über keinen Internetzugang verfügen, ist eng mit dem Status des E-Votings im Konzept der Stimmabgabe[34] verknüpft, also ob E-Voting als Ersatz zur herkömmlichen Wahl, als ergänzendes Angebot oder als Alternative zur Briefwahl eingeführt werden soll.

Die Einführung der Internetwahl als Regelfall begegnet durchgreifenden verfassungsrechtlichen Bedenken [vgl. Birkenmaier 2004, 113]. Nach der gegenwärtigen Verbreitung der privaten Internetanschlüsse würde fast die Hälfte der deutschen Bevölkerung vom Wahlvorgang ausgeschlossen, zumindest im individuellen Bereich [vgl. Eimeren et al. 2004, 351]. Doch auch wenn die Wahl in herkömmlichen Wahllokalen oder in Wahlkiosken per Internet stattfinden würde, kann die erforderliche Medienkompetenz nicht vorausgesetzt werden [vgl. Will 2002, 77]. Betrachtet man zusätzlich die soziodemographische Struktur der Internetnutzer, zeigt sich, dass laut der ARD/ZDF Online-Studie 2004 der typische Internetnutzer immer noch männlich, 20-39 Jahre alt, berufstätig und formal höher gebildet ist. Besonders die Nicht-Berufstätigen sowie Personen ab 50 Jahren sind weiterhin in großer Mehrheit offline; daraus wäre eine unzureichende Kenntnis im Bezug auf die Bedienung eines Wahlcomputers abzuleiten [vgl. Eimeren et al. 2004, 351]. Ein Teil der Bevölkerung wäre also auf Hilfe bei der Stimmabgabe angewiesen. Die Voraussetzungen für eine gültige Stimmabgabe bei Tätigwerden einer Hilfsperson sind laut § 33 Absatz 2 BWG jedoch auf einen „Wähler, der des Lesens unkundig ist oder durch körperliche Gebrechen gehindert ist [...] beschränkt." Im Wahllokal oder -kiosk hätte zwar der Großteil der Bürger Zugang zur Wahl, wäre aber aufgrund fehlender technischer Kenntnisse de facto vom Wahlvorgang ausgeschlossen.

Bei einer ausschließlichen Internetwahl müsste auch die Möglichkeit zur Briefwahl entfallen. Zwar besteht laut BVerfG kein verfassungsrechtlicher Anspruch auf die Einrichtung der Briefwahl [vgl. BVerfGE 12, 139 (142f.); 15, 165 (167)], jedoch würden so

[34] Zum Konzept der Stimmabgabe vgl. Kapitel 2.2.

alle wahlberechtigten Bürger von der Wahl ausgeschlossen, die nach § 25 Absatz 1 Bundeswahlordnung[35] einen anerkannten Hinderungsgrund haben, dessentwegen sie an der Wahl im Wahllokal nicht teilnehmen können und die zusätzlich nicht über einen Internetzugang verfügen. Eine ausschließliche Internetwahl scheidet unter dem Aspekt der Allgemeinheit der Wahl gemäß Artikel 38 GG somit aus. Zudem wird das Recht auf Teilnahme an der Wahl und somit an der demokratischen Willensbildung in liberal-demokratischen Staaten als Menschenrecht begriffen, unabhängig von persönlichen Leistungen oder Befähigungen [vgl. Wild 2003, 176].

Die Einführung des E-Votings neben der Abstimmung an der Urne im Wahllokal und der Briefwahl bietet dem Bürger eine dritte Möglichkeit (‚optionale Alternative'). Die fakultative Abstimmung im Internet könnte an individuellen Zugängen, an Wahlkiosken sowie im Wahllokal erfolgen. Die Möglichkeiten zur Wahlteilnahme würden also technisch erweitert [vgl. Hanßmann 2003, 117]. Im Zeitalter der wachsenden Mobilität, der Freizügigkeit und Niederlassungsfreiheit in der Europäischen Union ist die herkömmliche Briefwahl nach wie vor die einzige Möglichkeit für die Bürger, die sich am Wahltag nicht in ihrem Heimatwahlkreis aufhalten, trotzdem an Wahlen teilzunehmen. Die konstante Steigerung der Zahl der Teilnehmer an der Briefwahl verdeutlicht ein Interesse an flexibleren Möglichkeiten zur Stimmabgabe; zwischen 1990 und 2002 hat sich die Anzahl der Briefwähler auf 18% der Wähler fast verdoppelt [vgl. Der Bundeswahlleiter 2003, 4]. Doch die Beförderung der Wahlbriefe per Post trägt immer das Risiko einer verspäteten Zustellung. Wahlbriefe, die nicht bis 18.00 Uhr des Wahltages eingehen, können nicht als gültiges Votum gewertet werden[36].

Zusätzlich bietet die optionale Alternative körperlich behinderten oder eingeschränkten Menschen Vorteile gegenüber der klassischen Wahlmethode. Der Anteil der Schwerbehinderten in Deutschland beträgt 8, 1% der Bevölkerung, 80% der Menschen mit Behinderung nutzen bereits das Internet [vgl. Schmitz 2002, 1]. Selbst wenn von den behinderten Wahlberechtigten, die Zugang zum Internet haben, nicht alle auf die bisherige Hilfe nach § 32 Absatz 2 BWG verzichten könnten, würde durch die Einführung der optionalen Alternative dem Grundsatz der Allgemeinheit der Wahl in besonderer Weise Rechnung getragen. Die Wirkung der optionalen Alternative wird insofern weiter unterstützt, als dass nach § 11 Absatz 1 des Gesetzes zur Gleichstellung behinderter Men-

[35] Die Bundeswahlordnung wird im Folgenden als BWO bezeichnet.
[36] Siehe § 74, § 75 BWO und § 36 BWG.

schen (BGG) die Internetauftritte und –angebote öffentlicher Träger so gestaltet sein müssen, „dass sie von behinderten Menschen grundsätzlich uneingeschränkt genutzt werden können."

Da sich die Internetwahl fakultativ gestalten würde, bliebe die Möglichkeit zur klassischen Präsenzwahl sowie zur Briefwahl bestehen. Beachtet man jedoch die soziodemographische Struktur der Internetnutzer, muss davon ausgegangen werden, dass die Nutzung der Internetwahl nicht in allen Bevölkerungsschichten gleich wahrgenommen würde [vgl. Hanßmann 2003, 120]. Am Wahltag entscheiden verschiedene äußere Faktoren über die Höhe der Wahlbeteiligung, so z.B. auch das Wetter, das Internet- und Urnenwähler unterschiedlich betreffen würde [vgl. Will 2002, 79]. Somit hätten die Internetwähler, die im individuellen Bereich ihre Stimme abgeben könnten, einen leichteren Zugang zur Wahl, während Urnenwähler den Weg ins Wahllokal in Kauf nehmen müssten. Bezogen auf die soziodemographischen Unterschiede der Internetnutzer könnte dies zu Verzerrungen bei der Wahlbeteiligung und letztlich auch beim Ergebnis führen [vgl. Hanßmann 2003, 120].

Dem kann jedoch entgegengesetzt werden, dass die Möglichkeit der klassischen Stimmabgabe im Wahllokal bereits dem Allgemeinheitsgrundsatz entspricht. Die Möglichkeit zur Briefwahl steht rechtlich nur den Bürgern offen, die nach § 25 Absatz 1 BWO einen anerkannten Hinderungsgrund haben. Denkbar wäre eine ähnliche Regelung der Antragsstellung auch für die internetbasierte Wahlbeteiligung im individuellen Bereich. In diesem Fall kann der bloße Umstand, dass nicht alle Bürger über die technische Möglichkeit der Teilnahme an der optionalen Internetwahl verfügen, ebenfalls nicht dem Allgemeinheitsgrundsatz widersprechen.

Aufgrund der oben diskutierten Argumente, die gegen eine Substituierung des herkömmlichen Wahlvorgangs durch die Internetwahl sprechen, kann letztere auch die Briefwahl nicht komplett ersetzen. Bei Streichung der Briefwahl entfiele für die Bürger, die weder über einen Internetzugang noch die erforderliche Medienkompetenz verfügen, bei Verhinderung an der Präsenzwahl, auch die Möglichkeit zur Fernwahl. Die Einführung der Internetwahl als optionale Alternative zur Briefwahl ist mithin eine technische Erweiterung der Möglichkeiten zur Teilnahme an Wahlen. Sowohl Brief- als auch Internetwahl erfordern einen anerkannten Hinderungsgrund. Von welcher Option der Wähler Gebrauch macht, ist ihm überlassen. Diejenigen, die freiwillig die Internetwahl

in Anspruch nehmen, sind also auch für ihre erforderlichen technischen Kompetenzen grundsätzlich selbst verantwortlich [vgl. Hanßmann 2003, 123].

Prinzipiell ist der zeitliche Rahmen, in dem die Internetfernwahl vollzogen werden kann, zu erörtern. Der klassische Wahlbrief muss nach § 36 Absatz 1 BWG bis spätestens 18.00 Uhr des Wahltages beim Kreiswahlleiter eingehen; somit müssen Briefwähler ihre Wahlentscheidung im Vorfeld treffen. Demgegenüber ist eine internetbasierte Fernwahl theoretisch bis zur Schließung der Wahllokale technisch möglich. Dieser Aspekt kann als

> „eine letztlich wünschenswerte Annährung der Teilgruppe der Internetwähler aus der Gruppe der gemäß § 25 Absatz 1 BWO verhinderten Wähler an die Möglichkeiten der vom Gesetz als Regelfall vorgesehenen Urnenwähler“ [Will 2002, 82]

gesehen werden. Die relative Benachteiligung der Briefwähler bezüglich des zeitlichen Entscheidungsrahmens gegenüber Internetwählern widerspricht nicht dem Grundsatz der Allgemeinheit der Wahl, weil die maßstabbildende Urnenwahl ebenfalls eine Stimmabgabe bis 18.00 Uhr vorsieht.

Es kann festgehalten werden, dass die Substitution der klassischen Wahl durch E-Voting nicht vereinbar mit dem allgemeinen Wahlrecht ist. Eine fakultative Internetwahl als optionale Alternative im individuellen Bereich würde dem Grundsatz der Allgemeinheit der Wahl entsprechen, der durch die Beibehaltung der klassischen Präsenzwahl sowie die Möglichkeit zur Briefwahl gewahrt bliebe. Soweit der Grundsatz der Allgemeinheit der Wahl auch eine sicherheitstechnische Dimension aufweist, wird diese in Kapitel 2.4 näher erläutert.

2.3.2 Unmittelbare Wahl

Der Grundsatz der unmittelbaren Wahl beinhaltet, dass zwischen die Entscheidung des Wählers und die Zusammensetzung des gewählten Parlaments keine weitere Willensäußerung treten darf. Die Zwischenschaltung von Wahlmännern, die nach eigenem Ermessen die Abgeordneten wählen, ist somit nicht zulässig [vgl. Will 2002, 151]. Gemäß der Rechtssprechung des BVerfG soll das Volk das „letzte und entscheidende Wort“ [BVerfGE 3, 45 (49f.); 7, 63 (68)] bei der Wahl der Kandidaten haben. Nach der Stimmabgabe des Wählers darf nur noch die mathematische Ermittlung und Feststellung des Wahlergebnisses stehen [vgl. Schreiber 2002, 91]. Bezüglich dieser Anforderungen ergeben sich beim E-Voting im Vergleich zur herkömmlichen Wahl keine we-

sentlichen Unterschiede. Allein die sicherheitstechnischen Risiken wie Manipulation oder Fälschung der Voten können die Unmittelbarkeit der Wahl gefährden, jedoch nicht in dem o.g. Sinne. Die Sicherung des Einflusses des Volkes auf die Zusammensetzung der Parlamente ist Ziel der Unmittelbarkeit, somit kann die

> „Verletzung der Unmittelbarkeit der Wahl [...] demnach nur durch staatliches Verhalten erfolgen und wenn Private auf der Grundlage staatlicher Regelungen handeln“ [Hanßmann 2003, 136].

Fasst man dagegen auch die Höchstpersönlichkeit der Stimmabgabe unter den Grundsatz der Unmittelbarkeit[37], kann dieses Prinzip beim E-Voting, ähnlich wie bei der Briefwahl, nicht gänzlich gesichert werden. Es besteht die Gefahr, dass die Wahlhandlung durch Dritte vorgenommen wird, mag dies auch im Sinne des Wahlberechtigten geschehen. Selbst wenn die Verfassungskonformität der Briefwahl teilweise umstritten ist [vgl. Buchstein 2000a, 892 m.w.N.][38], hat das BVerfG die Briefwahl in Abwägung zwischen dem Allgemeinheitsgrundsatz und der Geheimhaltung für zulässig erklärt [vgl. Buchstein 2002, 57]. Somit sollte die Internetwahl bezüglich der Höchstpersönlichkeit der Stimmabgabe ebenfalls zulässig sein, zumal die persönliche Wahl beim E-Voting wie die Briefwahl durch eine dem § 36 Absatz 2 BWG entsprechende strafbewehrte Versicherung an Eides Statt geschützt werden kann.

2.3.3 Freie Wahl

Der Grundsatz der freien Wahl besagt, dass jeder Wahlberechtigte seinen Willen ohne Zwang ungehindert zum Ausdruck bringen kann. Somit umfasst der Grundsatz der freien Wahl auch das Recht, nicht oder bewusst ungültig zu wählen.

> „Die Freiheit der Wahl [besagt] daher, dass die Ausübung des Wahlrechts ohne (psychologischen) Druck, (physischen) Zwang oder sonstige unzulässige direkte oder indirekte Einflussnahme von außen erfolgen muss“ [Hanßmann 2003, 137f.].

Die Freiheit der Wahl steht in direktem Zusammenhang mit der geheimen Wahl. Denn nur wenn kein Zusammenhang zwischen Votum und Wähler hergestellt werden kann, ist die freie Wahl möglich und garantiert. Folglich ist mit der Einhaltung der geheimen Wahl auch eine freie Wahl gesichert. Der Grundsatz beinhaltet dennoch eine von der geheimen Wahl unabhängige Bedeutung, die über die eigentliche Stimmabgabe hinausgeht, da die in § 32 BWG bestimmte unzulässige Wahlbeeinflussung durch Wahlpropa-

[37] Vgl. z.B. [Will 2002], [Hanßmann 2003].
[38] Zur Diskussion zur Verfassungskonformität der Briefwahl vgl. [Schreiber 2002].

ganda sich auch auf die vorgelagerten Phasen des Wahlverfahrens bezieht [vgl. Birkenmaier 2004, 59]. Der unzulässige Druck, von staatlicher wie von privater Seite, gilt als beeinträchtigende Wahlbeeinflussung[39]. Nur im Rahmen der freien Meinungsäußerung ist die Wahlbeeinflussung durch Privatpersonen zulässig und im Prozess der politischen Meinungsbildung sogar als notwendig anzusehen [vgl. Hanßmann 2003, 138]. Dabei dürfen die strafrechtlichen Grenzen jedoch nicht überschritten werden.

Beim E-Voting ist der Freiheitsgrundsatz zum einen ähnlichen Gefährdungen wie bei der Briefwahl, zum anderen auch internetspezifischen Risiken ausgesetzt. Bei der herkömmlichen Präsenzwahl in der Wahlkabine kann davon ausgegangen werden, dass zumindest der unmittelbare Vorgang der Stimmabgabe frei von unberechtigter Einflussnahme möglich ist, vor allem durch die Gewährleistung der geheimen Stimmabgabe. Bei der Wahl im individuellen Bereich lässt sich eine derartige Beeinflussung des Wählers durch Dritte nicht ausschließen, dieses Risiko ist bei der Internetwahl ebenso hoch zu bewerten wie bei der Briefwahl. Bezogen auf die Briefwahl hat das BVerfG in seinen Entscheidungen von 1967[40] und 1981[41] jedoch zugunsten der Allgemeinheit der Wahl entschieden, auch wenn dadurch eine Gefährdung der freien und geheimen Wahl entstehen könnte. Dem Grundsatz der allgemeinen Wahl wird in besonderem Maße Rechnung getragen, da durch die Briefwahl auch den Bürgern eine Wahlmöglichkeit gegeben ist, die nach § 25 BWO einen anerkannten Hinderungsgrund haben [vgl. BVerfGE 59, 119 (125)]. Die Briefwahl ist somit nicht unbeschränkt zugelassen, sondern an Bedingungen geknüpft.

Wie die Briefwahl kann die Internetwahl außerhalb des Wahllokals stattfinden und ist somit den gleichen Risiken bezüglich der freien Wahl durch unzulässige Beeinflussung Dritter ausgesetzt. Denkbar ist jedoch eine Übertragung der Argumentation des BVerfG zur Abwägung zwischen Allgemeinheits- und Freiheitsgrundsatz auf das E-Voting [vgl. Will 2002, 119]. Zwar kann vertreten werden, dass die Einführung der Internetwahl nicht erforderlich sei, da die bestehende Briefwahl ja bereits dem Grundsatz der Allgemeinheit besonders entspricht [vgl. Buchstein 2000a, 901]. Das BVerfG hat in seinen Entscheidungen jedoch nicht geprüft, ob die Einführung der Briefwahl erforderlich ist, sondern ist davon ausgegangen, das dem Gesetzgeber bei der Ausgestaltung des Wahl-

[39] Vgl. § 108 Wählernötigung, § 108a Wählertäuschung und § 108b Wählerbestechung Strafgesetzbuch (StGB).
[40] Siehe BVerfGE 21, 200 (204f.).
[41] Siehe BVerfGE 59, 119 (124f., 126).

rechts nach Artikel 38 Absatz 3 GG zur Umsetzung der Vorgaben aus Artikel 38 Absatz 1 GG ein weiter Gestaltungsspielraum zusteht [vgl. BVerfGE 59, 119 (124)]. Des Weiteren wurde festgestellt, dass „nicht jeder der verfassungsrechtlich festgelegten Wahlrechtsgrundsätze in voller Reinheit verwirklicht werden kann“ [BVerfGE 59, 124]. Die Verantwortung liege bei dem Gesetzgeber; das BVerfG prüfe nur, ob dieser die Grenzen des im GG eingeräumten Gestaltungsspielraums nicht überschreite.

> „Das Bundesverfassungsgericht könne dieser Entscheidung nur entgegentreten, wenn sie mit einer übermäßigen Einschränkung oder Gefährdung der Grundsätze der unmittelbaren, freien, gleichen und geheimen Wahl verbunden wäre. Dies ist nicht der Fall“ [BVerfGE 59, 125].

Diese Rechtssprechung bezieht sich, wie oben erwähnt, nicht auf jede beliebige Form der Briefwahl, sondern nur auf die des BWG. Die Briefwahl ist also nicht für den Regelfall gedacht, sondern als Ausnahme neben der Präsenzwahl, deren Zulassung an die Beschränkungen des BWG gebunden ist [vgl. BVerfGE 21, 200 (205)]. Neben dem anzuerkennenden Hinderungsgrund ist der Wähler verpflichtet, nach § 36 Absatz 2 BWG den Wahlzettel unbeobachtet zu kennzeichnen und an Eides Statt zu versichern, dass der Stimmzettel persönlich bzw. im Sinne des Wählers gekennzeichnet wird. Im Falle einer Internetwahl im individuellen Bereich wäre davon auszugehen, dass das BVerfG für die verfassungsrechtliche Zulassung des E-Votings die jetzigen Regelungen des BWG zur bestmöglichen Sicherstellung der Wahlrechtsgrundsätze für erforderlich erklären würde [vgl. Hanßmann 2003, 142]. Bei der Internetfernwahl müsste zunächst ein Hinderungsgrund vom Wähler im Sinne des § 25 BWO glaubhaft gemacht werden. Die erforderliche eidesstattliche Versicherung wird im herkömmlichen Verfahren durch die eigenhändige Unterschrift geleistet, dies wäre beim E-Voting ohne Medienbruch nicht möglich. Das Signaturgesetz ist seit Mai 2001 in Kraft. Durch einen Zusatz in § 126a Bürgerliches Gesetzbuch[42] ist die qualifizierte Signatur der eigenhändigen Unterschrift weitgehend gleichgestellt, so dass die eigenhändige Unterschrift durch eine akkreditierte, elektronische Signatur[43] ersetzt werden kann.

Beim E-Voting können neben den o.g. Risiken für die Freiheit der Wahl auch internetspezifische Gefährdungen auftreten. Nach § 32 Absatz 1 BWG ist am Wahltag in, an und vor dem Wahllokal jede Art von Wahlpropaganda unzulässig. Dies umfasst die

[42] Das Bürgerliche Gesetzbuch wird im Folgenden als BGB bezeichnet.
[43] Die elektronische Signatur ist eine elektronische ‚Unterschrift’, die mit Hilfe von Verfahren der asymmetrischen Kryptographie erstellt wird. ‚Elektronische Signatur’ und ‚digitale Signatur’ werden im Folgenden synonym verwendet. Vgl. zum Verfahren Kapitel 2.4.3.1.3.

mögliche Beeinflussung der Wähler durch Wahlbewerber, Parteien, Wähler und andere Personen, Personengruppen und Institutionen [vgl. Schreiber 2002, 493]. Bei einer Wahl im individuellen Bereich, ob per Brief oder Internet, kann diese von Propaganda unbeeinflusste Stimmabgabe vom Staat nicht garantiert werden. Die Verantwortung liegt also beim Wähler[44] [vgl. Will 2002, 125]; er hat für eine freie Stimmabgabe Sorge zu tragen.

Im Falle einer Internetwahl wird es dem Wähler erschwert, sich von unzulässiger Wahlbeeinflussung freizuhalten. Die Wahlwerbung kann im Moment der Stimmabgabe durch Pop-Ups[45] oder Banner[46] auf dem Bildschirm des Wählenden erscheinen. Die offiziellen Wahlseiten sind von staatlicher Seite frei von jeder Beeinflussung, also unparteiisch, zu halten. Die Bildoberfläche muss allein der zentralen Bedeutung der Stimmabgabe gerecht werden, Werbebanner und Pop-Ups sind wahlrechtlich unzulässig [vgl. Buchstein 2000a, 891]. Diese können jedoch auch von anderen Internetseiten ausgelöst werden, die der Wähler eventuell zu Informationszwecken in seinem Browser gleichzeitig geöffnet hat. Denkbar wäre aufgrund dieser möglichen Gefährdung der freien Wahl eine Verpflichtung des Wählers, vor dem Wahlakt oder gleichzeitig mit diesem keine weiteren Internetseiten zu öffnen [vgl. Will 2002, 126] bzw. den Browser entsprechend einzustellen, so dass Pop-Ups nicht zugelassen werden. Dieses Vorgehen setzt allerdings Kooperation und technische Kenntnis des Benutzers voraus. Ein Werbeverbot von Seiten des Gesetzgebers für den Zeitraum der Wahl auszusprechen, ähnlich dem § 32 BWG, wäre aufgrund des weltweiten Zugangs und der Unkontrollierbarkeit des Internets nicht realisierbar. Die freiwillige Beeinflussung des Wählers im individuellen Bereich könnte also nicht ausgeschlossen werden, doch auch der Briefwähler kann sich aus freien Stücken Wahlpropaganda aussetzen. Allein wenn der Wahlberechtigte mit Sanktionen unter Druck gesetzt wird[47], greift das Gesetz. Wenn staatlicherseits gewährleistet wird, dass der Wähler sich der unfreiwilligen Beeinflussung entziehen kann, indem er z.B. während des Wahlvorgangs nur die offizielle Wahlseite öffnet, kann die Internetwahl unter dem Aspekt der freien, im Sinne von unbeeinflussten, Wahl als zulässig angesehen werden.

[44] Vgl. auch BVerfGE 59, 119 (126f.).
[45] Ein Pop-Up-Fenster ist ein Fenster mit Informationen, das bei bestimmten Mausaktionen aufklappt. Anbieter im WWW nutzen die Funktion, um Werbung im Webbrowser anzuzeigen.
[46] Ein Banner ist eine streifenförmige Werbeeinblendung und erstreckt sich typischerweise über die gesamte Bildschirmbreite. Oft enthalten Banner einen Link zu der beworbenen Seite.
[47] Vgl. § 108 Wählernötigung, § 108a Wählertäuschung und § 108b Wählerbestechung StGB.

Der Grundsatz der freien Wahl beinhaltet neben der unbeeinflussten Stimmabgabe auch die Freiheit, nicht bzw. ungültig zu wählen. Die Abgabe einer bewusst ungültig abgegeben Stimme kann als eine wesentliche demokratische Willensäußerung gewertet werden [vgl. Schreiber 2002, 93]. Durch die technischen Gegebenheiten des Internets kann dies jedoch nicht auf dem Weg geschehen wie beim herkömmlichen Stimmzettel, d.h. durch schriftliche Willensäußerung oder durch Nichtkennzeichnung. Zur Stimmenthaltung könnte ein Button ‚ungültig wählen' auf dem elektronischen Stimmzettel angebracht werden[48]. Zu bedenken ist bei dieser Form allerdings, dass der Internetstimmzettel damit deutlich vom herkömmlichen abwiche und der Wähler durch diese ausdrückliche Option erst animiert werden könnte, ein ungültiges Votum abzugeben [vgl. Hanßmann 2003, 148]. Eine weitere Möglichkeit wäre eine generelle Plausibilitätskontrolle des Stimmzettels. Im Falle eines ungültigen Votums, z.B. durch Aktivierung von zu vielen oder keinem der Wahlvorschläge, würde der Wähler auf seinen vermeintlichen Fehler aufmerksam gemacht und könnte sein Votum gegebenenfalls korrigieren. Durch eine einfache Bestätigung nach dem ausdrücklichen Hinweis, dass die Stimme nach § 39 BWG ungültig gewertet wird, wäre eine bewusst ungültige Wahl möglich. Eine derartige Plausibilitätskontrolle wahrt zum einen die Freiheit der Stimmabgabe, zum anderen kann die Anzahl der unbewusst ungültig abgegeben Stimmen reduziert werden [vgl. Birkenmaier 2004, 60].

Nicht unproblematisch ist dieser Vorschlag jedoch im Hinblick auf die Gleichheit der Wahl, da weder eine Plausibilitätskontrolle noch der Hinweis auf ein ungültig abgegebenes Votum bei den herkömmlichen Wahlmöglichkeiten gegeben ist. Bei Beachtung der genannten Aspekte jedoch kann die Internetwahl dem Grundsatz der freien Wahl nicht widersprechen.

2.3.4 Gleiche Wahl

Der Grundsatz der gleichen Wahl bezieht sich sowohl auf die Wahlberechtigten als auch auf die Wahlbewerber und steht in engem Zusammenhang mit dem Grundsatz der Allgemeinheit der Wahl. Während sich die allgemeine Wahl auf den Einfluss aller wahlberechtigten Bürger bezieht, also die allgemeine, gleiche Stimmberechtigung, garantiert die gleiche Wahl, dass jeder Wahlstimme das gleiche Stimmgewicht zukommt

[48] So realisiert bei der Wahl zum Studierendenparlament der Universität Osnabrück. Vgl. hierzu Kapitel 3.4.1.

[vgl. Zippelius 2003, 211]. Nach ständiger Rechtssprechung des BVerfG besagt der Gleichheitsgrundsatz, „dass jedermann sein Wahlrecht in formal möglichst gleicher Weise [..] ausüben können [soll]“ [BVerfGE 16, 138]. Alle Wähler müssen also den gleichen Einfluss auf das Wahlergebnis haben, d.h. dass jeder Wähler über die gleiche Stimmanzahl verfügen muss und jede Stimme – zumindest bei der Verhältniswahl – bei der Zuteilung der Parlamentssitze berücksichtigt wird [vgl. Will 2002, 100]. Neben dieser Zähl- und Erfolgswertgleichheit müssen zudem auch die gleichen Erfolgschancen für Kandidaten gewährleistet sein.

Der Grundsatz der Gleichheit der Stimmen erfordert auch von E-Voting-Systemen die technische Gewährleistung, dass jeder Wähler seine Stimme tatsächlich nur einmal abgeben kann. Die Garantie der Stimmengleichheit umfasst auch die Verhinderung von Wahlfälschungen und unbewussten Fehlern bei der Stimmenauszählung [vgl. BVerfGE 85, 148 (157)]. Der Gesetzgeber ist also dazu verpflichtet, den Gleichheitsgrundsatz auch vor einer Wahlfälschung zu schützen.

Bei der klassischen Wahl im Wahllokal erfolgt die Identifizierung des Wählers durch Vorzeigen der erhaltenen Wahlbenachrichtigung und den Abgleich des Namens im Wählerverzeichnis, gegebenenfalls durch Vorlage seines Personalausweises[49]. Die Stimmabgabe wird im Wählerverzeichnis registriert, pro Wähler nur ein Stimmzettel ausgegeben und so eine erneute Stimmabgabe verhindert. Bei der Briefwahl wird nach § 30 BWO die Mehrfachwahl ausgeschlossen, indem nach der Erteilung des Wahlscheins im Wählerverzeichnis ein Vermerk über die Stimmabgabe per Wahlschein gemacht wird. Der betroffene Wähler kann dann nur noch per Wahlschein wählen, gegebenenfalls auch im Wahllokal [vgl. Schreiber 2002, 526]. Hierbei würde der Wahlschein einbehalten werden, so dass eine zweite Stimmabgabe unmöglich ist, da ein Vermerk im Wählerverzeichnis das Vorlegen des Wahlscheins zur Stimmabgabe erforderlich macht [vgl. Birkenmaier 2004, 65]. Bei der Briefwahl kann jedoch nicht sichergestellt werden, dass Personenidentität zwischen dem erfolgreichen Antragsteller und dem Wähler besteht. Selbst bei Kenntnis des eigentlich Stimmberechtigten führt dies zur Verletzung des Gleichheitsgrundsatzes, da es sich hierbei um eine Form der mehrfachen Stimmabgabe im individuellen Bereich handelt [vgl. Will 2002, 102]. Dieser Gefahr wird mit

[49] Vgl. § 56 Absatz 3 BWO.

Strafandrohung gemäß § 156 StGB begegnet, der eine mehrfache Stimmabgabe nicht gänzlich ausschließt, aber dennoch den Grundsatz der gleichen Wahl schützt.

Auf eine internetgestützte Präsenzwahl im Wahllokal kann die Regelung der herkömmlichen Präsenzwahl übertragen werden; die Identifizierung erfolgt entsprechend § 56 Absatz 3 BWO durch das Vorlegen der Wahlbenachrichtigung und den Abgleich des Wählerverzeichnisses. Da das E-Voting jedoch nur als optionale Alternative eingeführt werden kann[50], müsste auch der Internetfernwähler einen Antrag stellen [vgl. Birkenmaier 2004, 68]. Das Verfahren könnte ähnlich dem der Briefwahl vollzogen werden, sollte aber zur Vermeidung des Medienbruchs auch online durchgeführt werden können[51]. Bei der Registrierung als Online-Wähler müsste ein Vermerk, entsprechend dem oben erwähnten Briefwahlvermerk, eine zweite Wahl im Wahllokal verhindern. Problematisch wäre diese Lösung jedoch bei den Wählern, die sich spontan doch für die Präsenzwahl entscheiden bzw. im individuellen Bereich entweder technische Schwierigkeiten bei der Stimmabgabe haben oder keine freie und geheime Wahl durchführen können [vgl. Hanßmann 2003, 152f.]. Eine mögliche Lösung wäre die Gewährung des Zugriffs auf die einzelnen digitalisierten Wählerverzeichnisse durch den hierzu autorisierten Wahlvorstand.

Um eine höchstpersönliche Abgabe des Votums beim E-Voting außerhalb des Wahllokals zu garantieren, sind verschiedene Sicherheitsmaßnahmen zur Identifizierung des Wählers erforderlich. Dies kann zum einen durch ein PIN[52]/TAN[53]-Verfahren ähnlich dem Online-Banking realisiert werden. Bei dieser Möglichkeit ist zu gewährleisten, dass die jeweilige Kennung dem Wahlberechtigten sicher und geheim zukommt. Nach der Stimmabgabe kann nicht mehr überprüft werden, ob der berechtigte Bürger auch tatsächlich persönlich gewählt hat. Zudem liegt dem Einsatz von PIN/TAN-Verfahren lediglich ein vertraglicher Rechtsrahmen zugrunde; die numerischen Eingaben sind der handschriftlichen Unterschrift rechtlich nicht gleichgestellt [vgl. Rüß 2002, 45]. Somit ist auch hier eine Form der Versicherung an Eides Statt nötig. Eine schriftliche Form im

[50] Vgl. Kapitel 2.3.1 zur allgemeinen Wahl.
[51] Es existieren bereits Online-Anträge für die herkömmliche Briefwahl, z.B. in der Stadt Berlin. Die vom Nutzer in einen Antrag im HTML-Format eingegebenen Daten werden verschlüsselt an die Geschäftsstelle des Landeswahlleiters geschickt und von dort an das zuständige Bezirkswahlamt weitergeleitet. Vgl. [N.N. 2002a].
[52] Eine Persönliche Identifikationsnummer (PIN) ist eine Geheimzahl, mit der man sich gegenüber einer Maschine ausweisen kann.
[53] Eine Transaktionsnummer (TAN) ist ein Einmalpasswort. Sie gilt quasi als Unterschrift und verfällt nach einmaligem Gebrauch.

herkömmlichen Sinne kommt nicht in Betracht, da dann der Internetwähler auch die klassische Briefwahl nutzen könnte [vgl. Will 2002, 103]. Sinnvoll ist daher allein die Verwendung der elektronischen Signatur[54]. Zwar vermag auch die elektronische Signatur Personenidentität zwischen Antragsteller und Wähler nicht vollständig zu gewährleisten, dies ist jedoch auch bei der gängigen Versicherung an Eides Statt nicht anders [vgl. Hanßmann 2003, 154].

Bezüglich des passiven Wahlrechts beinhaltet der Grundsatz der gleichen Wahl auch die gleichen Erfolgschancen für Wahlbewerber. Eine ungerechtfertigte Benachteiligung oder Begünstigung ist somit nicht zulässig. § 30 Absatz 1 BWG besagt, dass die Stimmzettel amtlich hergestellt werden. Dies erfolgt neben Rationalisierungserwägungen vor allem auch im Interesse der Einheitlichkeit [vgl. Schreiber 2002, 480]. Allen Wahlvorschlägen muss also der gleiche Raum auf dem Stimmzettel eingeräumt werden. Daraus resultiert die entsprechende Anforderung an den elektronischen Stimmzettel: alle Wahlbewerber müssen für den Wähler gleichermaßen sichtbar sein. Dies gilt auch bei verschiedenen Systemeinstellungen (z.B. Bildauflösung) und Monitorgrößen. Bereits bei herkömmlichen Stimmzetteln wird eingeräumt, dass die Wahlbewerber der ersten Plätze wahlpsychologisch im Vorteil sind [vgl. BVerfGE 29, 154 (164)]. Es ist naheliegend, diese Vermutung auf das E-Voting zu übertragen. Da sich laut § 30 Absatz 3 Satz 1 BWG die Reihenfolge der Landeslisten auf dem Stimmzettel nach den Erfolgen der letzten Bundestagswahl richtet, könnten insbesondere kleinere und weniger erfolgreiche Parteien erst durch Herab-Scrollen[55] zu sehen sein. Bedenkt man, dass Stimmzettel bei Kommunalwahlen die Größe eines DIN A1-Bogens haben können [vgl. Birkenmaier 2004, 62], ist jedoch fraglich, ob eine Darstellung zu gewährleisten ist, bei der alle Wahlbewerber auf einer Bildschirmgröße abgebildet und trotzdem lesbar sind[56].

Trotz Anerkennung des wahlpsychologischen Vorteils der Wahlbewerber, die auf den ersten Plätzen der Stimmzettel angeordnet sind, wird ihm mit der Begründung, dass sich die Wähler regelmäßig nicht von den Ordnungszahlen auf dem Stimmzettel beeinflussen lassen, sondern von parteipolitischen Zielen und von einzelnen Wahlbewerbern, aus rechtlicher Sicht kein besonderes Gewicht beigemessen [vgl. Schreiber 2002, 485f.

[54] Zum Verfahren der elektronischen Signatur siehe 2.4.3.1.3.
[55] Scrollen bezeichnet das horizontale oder vertikale Verschieben des Bildschirminhalts, um zu einem anderen Bereich des Dokuments zu gelangen.
[56] Ein menügesteuerter Wahlzettel ist aber aufgrund der erforderlichen Medienkompetenz und des Grundsatzes der Allgemeinheit der Wahl auszuschließen.

m.w. N.]. Wenn daher ausdrücklich und eindeutig darauf hingewiesen wird, dass es sich bei dem Angezeigten nur um einen Ausschnitt handelt, haben die Wähler nicht nur die Möglichkeit, sondern auch die erforderliche Information, um alle Wahlbewerber in ihre Entscheidung mit einzubeziehen.

Eine Gefahr für die Zähl- und Erfolgsgleichheit stellt das Risiko der Manipulation durch Dritte bei der Stimmabgabe, Übertragung und Auszählung dar. Dies ist auch in wahlentscheidendem Umfang möglich [vgl. Forschungsgruppe Internetwahlen 2002, 14]. Vor diesen Gefahren bietet auch die Wahlprüfung[57] allein keinen Schutz, da dieses Verfahren Zweifel an der Richtigkeit der Wahlen voraussetzt. Falls aber Anhaltspunkte für elektronische Wahlmanipulation fehlen, lässt sich der Wahlbetrug nicht aufdecken. Soweit die gleiche Wahl auch eine sicherheitstechnische Dimension aufweist, indem der Stimmzettel, der beim E-Voting aus elektronischen Daten besteht, manipuliert wird, wird dies in Kapitel 2.4 diskutiert.

2.3.5 Geheime Wahl

Die Einhaltung der geheimen Stimmabgabe bei politischen Wahlen gehört nach heutigem Verständnis zu den Kernelementen demokratischer Staaten[58] und umfasst den gesamten Wahlvorgang. Die geheime Wahl garantiert den Schutz der demokratischen Selbstbestimmung des Wählers, denn nur die Geheimhaltung der Stimmabgabe kann die uneingeschränkte Wahlfreiheit garantieren [vgl. Schreiber 2002, 141]. Sinn und Zweck der geheimen Stimmabgabe ist also die Sicherung des Grundsatzes der Freiheit der Wahl [vgl. Zippelius 2003, 202]. Voraussetzung hierfür ist das unbeobachtete Kennzeichnen des Stimmzettels sowie die Entkopplung der Wähleridentität von seinem Votum.

Um diese Geheimhaltung zu gewährleisten ist zum einen der Staat verpflichtet, Vorkehrungen zu treffen[59]. Zum anderen ist die Einhaltung der geheimen Wahl eine Rechtspflicht aller Teilnehmer einer Wahl[60]. Der Wähler *darf* nicht, er *muss* geheim wählen [vgl. Schreiber 2002, 500]. Die Geheimheit der Wahl ist somit nach dem deutschen Verfassungsverständnis obligatorisch. Wäre die Wahrung des Grundsatzes fakultativ,

[57] Vgl. Artikel 41 GG.
[58] Zur wahlrechtshistorischen und ideengeschichtlichen Dimension des Wahlrechtsgrundsatzes der geheimen Wahl vgl. [Buchstein 2000b].
[59] Vgl. § 50, § 51, § 52 BWO über die Beschaffenheit von Wahlzellen, -urnen und –tischen.
[60] Die Verletzung des Wahlgeheimnisses ist strafbar nach § 107c StGB.

würde dies allein eine Gefährdung der freien Wahl bedeuten. Der Wähler könnte unter Druck gesetzt werden, auf die geheime Stimmabgabe zu verzichten und wäre somit erpressbar. Der einzelne Wähler darf zwar nach der Stimmabgabe sein Votum öffentlich preisgeben, jedoch darf dies nie Gegenstand einer Überprüfung sein. Ob die öffentliche Aussage des Wählers seinem tatsächlichen Votum entspricht, ist nicht nachvollziehbar und somit Kern des Wahlgeheimnisses [vgl. Buchstein 2000a, 898]. Folglich muss ein E-Voting-System derartig gestaltet sein, dass trotz eindeutiger Identifizierung des Wählers eine Kenntnisnahme oder spätere Rekonstruktion seines Votums bzw. Rückschlüsse auf seine Person nicht möglich sind. Bei klassischen Wahlen im Wahllokal wird dies durch die Entkopplung von Identifizierung des Wählers durch die Wahlhelfer einerseits und geheimer Abstimmung andererseits erreicht. Durch die Vermischung der gleichgestalteten Stimmzettel in der Urne ist beim Auszählen keine Zuordnung der Stimmen mehr möglich. Dies führt

> „zur Auflösung des kontradiktorischen Verhältnisses von Geheimheits- und Gleichheitsgrundsatz in einer beide, voll verwirklichenden Weise“ [Birkenmaier 2004, 90].

Bei der Briefwahl erfolgt die Identifizierung des Wählers mittels Wahlschein, der nach § 36 Absatz 1 BWG Teil des Wahlbriefes sein muss. Der Stimmzettel ist in einem gesonderten, verschlossenen Umschlag ebenfalls Teil des Wahlbriefes. Nach dem Abgleich des Wahlscheins mit dem Wählerverzeichnis wird dieser Umschlag nach § 75 Absatz 1 BWO ungeöffnet in die Urne gelegt. Somit ist eine Zuordnung nicht möglich. Bedenkt man, dass die Briefwahl dem Wähler die Wahl ermöglichen soll, der nicht an der Präsenzwahl teilnehmen kann, beinhaltet dies, dass der Ort der Stimmabgabe dem Briefwähler frei überlassen bleibt. Aufgrund dessen kann die Briefwahl als „privatisierter Wahlakt“ [Schreiber 2002, 522] bezeichnet werden. Insofern kann die Einhaltung des Geheimhaltungsgrundsatzes nicht staatlich gewährleistet werden [vgl. Birkenmaier 2004, 92]. Die Entscheidungen des BVerfG zugunsten der Briefwahl[61] bestätigen die zulässige Übertragung der Verantwortung vom Staat auf den Briefwähler, selbst für die Einhaltung des Wahlgeheimnisses zu sorgen. Durch die Glaubhaftmachung von Gründen[62] und die Versicherung an Eides Statt[63] ist die Briefwahl als Ausnahme zur Präsenzwahl zu sehen. Somit ist die Förderung des Wahlrechtgrundsatzes der Allgemein-

[61] Vgl. zu den BVerfGE Kapitel 2.3.3. Fn. 40 und Fn. 41.
[62] § 25 BWO.
[63] § 39 Absatz 4 Satz 6 BWG.

heit gegenüber der Geheimhaltung als vorrangig zu bewerten, solange das Verhältnis zwischen Brief- und Präsenzwähler deutlich zugunsten der Präsenzwähler ausfällt [vgl. Buchstein 2000a, 893].

Beim E-Voting kann das Spannungsverhältnis zwischen eindeutiger Identifikation des Wählers und Anonymität des Votums durch den Einsatz der elektronischen Signatur in ähnlicher Weise gelöst werden wie bei der Briefwahl. Zusätzlich ist eine ‚digitale Gewaltenteilung' erforderlich[64]. Das Prinzip der Gewaltenteilung ist implizit auch in der klassischen Wahl enthalten und wird durch die Anordnung der Kompetenzen, z.B. durch die personelle Aufgabentrennung bezüglich des Abgleichs mit dem Wählerverzeichnis, der Ausgabe der Stimmzettel etc., geregelt. Beim E-Voting kann der registrierende Server von dem auszählenden getrennt werden [vgl. Philippsen 2002, 142ff.]. Diese Trennung soll eine Zuordnung der Wählerstimme unmöglich machen. Wird diese Art der digitalen Gewaltenteilung kombiniert mit verschiedenen Sicherheitsverfahren[65], kann von einer sicheren Entkopplung der Identität des Wählers von seinem Votum ausgegangen werden.

Bezüglich der Gewährleistung der geheimen Stimmabgabe ergibt sich beim E-Voting im individuellen Bereich ein ähnliches Problem wie bei der Briefwahl[66]. Bei einer internetbasierten Präsenzwahl könnten dagegen die Regelungen nach § 35 BWG für die Stimmabgabe mittels Wahlgerät angewandt werden. So müssen die Geräte wie die klassischen Wahlkabinen vor den Blicken Dritter geschützt sein. Die Möglichkeit, Rückschlüsse auf das Wahlverhalten aufgrund von Armbewegungen beim Drücken eines Knopfes o.ä. ziehen zu können, wäre verfassungswidrig [vgl. Hanßmann 2003, 167].

Bei der Internetfernwahl kann die Einhaltung des Grundsatzes der geheimen Wahl nicht staatlich gewährleistet werden. Vorschläge, den individuellen Bereich um private Computer durch Kameras zu überwachen, scheitern nicht nur aus Datenschutz-, sondern auch Organisationsgründen[67]. Sie würden die Flexibilität des E-Votings ins Gegenteil umkehren, da die grundsätzlich flexiblere Stimmabgabe dann nur an den vorher angegeben Computern möglich wäre [vgl. Birkenmaier 2004, 107].

[64] Zur technische Realisierung der digitalen Gewaltenteilung vgl. Kapitel 2.4.3.5.4.
[65] Zu den technischen Schutzmöglichkeiten vgl. Kapitel 2.4.3.
[66] Zum Problem der mangelnden öffentlichen Kontrollmöglichkeit der Fernwahl vgl. Kapitel 2.3.3 zur freien Wahl.
[67] Vgl. ausführlicher [Buchstein 2000a], [Buchstein 2002].

Die Einführung der Internetfernwahl als alleiniges Wahlverfahren verstieße, unabhängig von der technischen Sicherheit, gegen den Wahlrechtsgrundsatz der geheimen Wahl, da die Wahrung des Grundsatzes nicht allgemein gewährleistet werden könnte [vgl. Buchstein 2000a, 901]. In Einklang mit geltendem Recht stünde die Internetfernwahl in Form der optionalen Alternative, wenn die Zulässigkeitsvoraussetzungen der Briefwahl angewandt würden. Hinsichtlich der Förderung der Allgemeinheit der Wahl kann die Rechtssprechung des BVerfG auf das E-Voting übertragen werden. Zu bedenken ist jedoch, dass die Urteile von 1967 und 1981[68] im Hinblick auf die Regelung der Briefwahl als Ausnahme zum Regelfall der Präsenzwahl gefällt wurden. Die Anzahl der Briefwähler ist seit dieser Zeit stark angestiegen. Bei den Bundestagswahlen 1965 nutzten 7, 3% der Wähler die Möglichkeit der Briefwahl, 1980 bereits 13%. Bei den letzten Bundestagswahlen 2002 wuchs die Zahl auf 18% bundesweit [vgl. Der Bundeswahlleiter 2003, 4]; in Wahlkreisen einiger Großstädte sogar auf über 30% [vgl. Kersting 2004, 18]. Zudem ist eine weitere Zunahme der Zahl der Fernwähler zu erwarten, wenn die Möglichkeit des E-Votings eingeführt würde [vgl. Buchstein 2000a, 900]. Die Anzahl der Wähler, deren geheime Stimmabgabe nicht öffentlich garantiert werden könnte, würde weiter wachsen und somit wohl nicht mehr als Ausnahme im Sinne der Rechtsprechung des BVerfG gelten. Während Kritiker diesen Umstand als verfassungsrechtlichen Hinderungsgrund zur Einführung der Internetfernwahl[69] sehen, ist andererseits die besondere Verwirklichung des Grundsatzes der Allgemeinheit hervorzuheben. Inwieweit das BVerfG seine Rechtssprechung in diesem Sinne weiterentwickelt, bleibt abzuwarten.

2.4 Sicherheitstechnische Anforderungen

2.4.1 Grundproblem Internetsicherheit

Die Frage, ob das Internet grundsätzlich für politische Wahlen geeignet ist, ist hauptsächlich eine Frage der Technik. Selbst wenn alle Voraussetzungen von staatlicher Seite geschaffen werden, um den demokratietheoretischen Anforderungen zu genügen, hängt eine gelungene Wahl allein von dem Sicherheitsgrad des Systems ab. Sicherheit bedeutet im Fall von E-Voting die technische Gewährleistung der Einhaltung der Wahlrechtsgrundsätze, die durch den Verlust an Vertraulichkeit, Integrität und Authentizität der

[68] Vgl. zu den BVerfGE Kapitel 2.3.3 Fn. 40 und Fn. 41.
[69] Vgl. z.B. [Buchstein 2000a], [Birkenmaier 2004]. Kritisch [Schreiber 2002].

Daten sowie die Verfügbarkeit des Systems gefährdet werden könnten. Die Sicherheit des Systems bezieht sich hier nicht allein auf die Sicherheit einzelner Computer, sondern vor allem auf die Sicherheit in Netzwerken, im Fall vom E-Voting also auf das Internet. Ein Computer wird in dem Moment unsicher, in dem er an ein Netzwerk angeschlossen wird [vgl. Schneier 2000, 169]. Ohne die Verbindung ist jedoch der Austausch und die Übertragung von Daten nicht möglich. Somit macht das Internet als Netzwerk E-Voting erst möglich, zum anderen birgt es auch eine große Gefahr.

Das Internet ist dezentral organisiert, d.h. es gibt keinen Zentralrechner, keinen zentralen Internet-Knoten, der als Schnittstelle zwischen großen Rechnernetzen dient, sowie keinen Ort, an dem alle Verbindungen zusammenlaufen. Diese Organisationsstruktur sorgt zum einen für eine sehr hohe Ausfallsicherheit, da so für die Kommunikation zwischen Nutzern meistens mehrere Kommunikationswege existieren, zum anderen schließt es eine übergeordnete zentrale Steuerungsinstanz auch geradezu aus. Die Gewährleistung einheitlicher Regelungen und rechtlicher Vorschriften ist schwierig durchzusetzen und zu kontrollieren [vgl. Birkenmaier 2004, 41].

Das Internet verbindet als ‚Netz der Netze' [Leib 1998, 85] verschiedene Netzwerke; zur Kommunikation dienen weltweit standardisierte Protokolle. Weit verbreitet sind die Protokolle IP (Internet Protocol), das die zu übertragenden Daten in Pakete aufteilt, adressiert und schließlich wieder zusammenführt, und TCP (Transmission Control Protocol), das den Datentransport überwacht und Übertragungsfehler korrigiert. Sie werden zu TCP/IP zusammengefasst[70]. Die Standardisierung der Adressierung und des Datenaustauschs zwischen verschiedenen Computern und Netzwerken ermöglicht eine von den verwendeten Betriebssystemen und Netzwerktechnologien unabhängige Kommunikation. TCP ist ein verbindungsorientiertes Protokoll, beim Aufbau einer Verbindung werden daher zwischen Server und Client[71] verschiedene Kontrollpakete ausgetauscht, um sich über den Zustand der TCP-Verbindung zu einigen [vgl. Fuhrberg 2000, 79].

Um die gezielte Übertragung von Nachrichten und Daten zu ermöglichen, ist jedem mit dem Netzwerk verbundenen Computer eine numerische IP-Adresse zugeordnet, durch die die einzelnen Rechner identifiziert werden. Stellvertretend hierfür steht in der Regel

[70] Zu den Techniken der Datenübertragung im Internet ausführlich vgl. [Fuhrberg 2000, 5ff.].
[71] Ein Client-Server-System besteht aus einem Client, der eine Verbindung mit einem Server aufbaut. Der Client bietet die Benutzeroberfläche oder die Benutzerschnittstelle der Anwendung an. Der Server stellt die Funktionalität zur Verfügung.

ein für sich sprechender Hostname[72]. Er wird im Rahmen des verwendeten Übertragungsprotokolls TCP/IP vom Domain Name Service (DNS) in die IP-Adresse umgewandelt.

Zur Übertragung werden die Daten in Pakete zerlegt, unabhängig voneinander verschickt und beim Empfänger wieder zusammengesetzt. Dabei können die einzelnen Pakete auf verschiedenen Wegen zu ihrem Zielpunkt gelangen, wodurch Netzausfälle oder –überlastungen kompensiert werden. An den Verbindungen zwischen den einzelnen Teilen eines Netzwerks oder zwischen vollständigen Netzwerken stehen sogenannte Router (‚Wegweiser'), die für die Weiterleitung der Pakete zuständig sind. Anhand von Streckentabellen und der Zieladresse bestimmen sie, auf welchem Weg ein Datenpaket am besten übermittelt wird. Aufgrund der globalen dezentralen Netzstrukturen muss dieser Datentransport nicht zwangsläufig über nationale Netze verlaufen.

Die Idee zur Vernetzung von Rechnern ist ursprünglich für einen kleinen Benutzerkreis konzipiert worden[73]. Bei der Entwicklung der verwendeten Protokolle stand zunächst die ungehinderte Kommunikation im Vordergrund, nicht die Sicherheit. Die Protokolle bilden noch immer die Basis der Kommunikation im Internet. Da dessen Ausmaß und Bedeutung sich jedoch grundlegend gewandelt haben, kann die offene, d.h. unverschlüsselte Datenübertragung heute als sicherheitsrelevanter Konzeptionsfehler bezeichnet werden [vgl. Fuhrberg 2000, 49]. Die unverschlüsselten Daten können an den Netzknoten ebenso wie in den Leitungen mitgelesen oder verändert werden. Beim E-Voting besteht so die Möglichkeit, das Wahlergebnis auf vielfältige Weise zu manipulieren: Stimmen können durch Hacker[74] und bösartige Softwareprogramme abgefangen, modifiziert, vervielfältigt oder zerstört werden. Ferner kann ein kompletter Zusammenbruch der Kommunikation herbeigeführt werden [vgl. Forschungsgruppe Internetwahlen 2002, 14].

Zusätzlich zu den Konzeptionsfehlern erleichtern oft auch sicherheitsrelevante Programmierfehler in der Software sowie Fehler in der Konfiguration, d.h. eine falsche

[72] Z.B. steht die Adresse www.rz.uni-hildesheim.de für die numerische IP-Adresse 147.172.16.46. Vgl. http://www.uni-hildesheim.de/de/3090.htm (Verifizierungsdatum: 16.09.2005).
[73] Den Ursprung des Internets bildet das ARPANET, das zunächst militärischen Forschungszwecken in den USA diente. Zur Entwicklung des ARPANET vgl. z.B. [Hörisch 2001, 372ff.].
[74] Als Hacker wird allgemein eine Person bezeichnet, die in der Lage ist, beliebige Schutzmaßnahmen gegen das Ausspähen von Daten und Kopieren von Daten in Netzwerken oder auf Datenträgern zu umgehen [Brockhaus 2003, 404].

Einstellung interner und externer Komponenten eines Systems, den Angreifern den Zugang über das Internet auf einen bestimmten Computer [vgl. Fuhrberg 2000, 57].

Durch die unterschiedlichen Angriffe entsteht ein Verlust an Vertraulichkeit, Integrität und Authentizität der Daten. Die Verfügbarkeit eines Systems kann durch eine Überlastung der vorhandenen Ressourcen gefährdet werden [vgl. Fuhrberg 2000, 54ff.]. Der Nutzer kann objektiv nicht überprüfen, ob seine verschickten Daten tatsächlich in der ursprünglichen Form bei dem Empfänger ankommen, noch weiß er, ob die von ihm empfangenen Daten gefälscht sind bzw. von einer gefälschten IP-Adresse stammen. So kann beim E-Voting ein Stimmzettel auf verschiedenen Bildschirmen zwar ähnlich aussehen, aber an entscheidender Stelle unterschiedlich und damit für den Wähler unerkennbar manipuliert sein. Dies ist gerade bezüglich der geheimen und gleichen Stimmabgabe von Bedeutung.

2.4.2 Angreifer und Angriffsformen

Sobald ein Computer an das weltweite Netz angeschlossen ist, können Angreifer versuchen, Zugang zu dem System zu erhalten.

> „Verbrechen im Cyberspace beinhalten alles, was man aus der physischen Welt kennt: Diebstahl, Schutzgelderpressung, Vandalismus, Voyeurismus, Missbrauch, Erpressung, Schwindel, Betrug“ [Schneier 2000, 12].

Angreifertypen unterscheiden sich also aufgrund ihrer Motivation und ihres Organisationsgrads[75]. Eine nationale Internetwahl hat für Angreifer, die aus finanziellen oder politisch motivierten Gründen handeln, sicher einen „ganz besonderen Charme“ [Birkenmaier 2004, 85]. Dies gilt für externe Angreifer über das Internet wie für interne Angreifer, z.B. zugangsberechtigte Systemadministratoren, gleichermaßen. Betroffen ist der gesamte Wahlvorgang: der direkte Abstimmungsvorgang auf der Client-Seite, die Übermittlung der Daten, die Verarbeitung auf der Server-Seite sowie die Speicherung der eingegangen Wahlstimmen.

2.4.2.1 Denial-of-Service-Angriff (DoS)

Ein Denial-of-Service-Angriff (‚Verweigerung des Dienstes’) zielt auf die Grundvoraussetzung zur Datenübertragung ab: die Verfügbarkeit des Servers. Ziel ist es, den attackierten Rechner zum Absturz zu bringen, indem die vorhandenen Ressourcen (An-

[75] Zur ausführlichen Beschreibung der Angreifer siehe z.B. [Schneier 2000], [Wiltner 2003].

zahl an Verbindungen, Rechenzeit, Bandbreite) durch falsche Verbindungsanfragen voll ausgeschöpft werden [vgl. Wiltner 2003, 89].

Eine verschärfte Variante des DoS-Angriffs ist der Distributed Denial-of-Service-Angriff (DDoS), der verteilte Angriff. Hierbei werden die Anfragen nicht von einem, sondern von mehreren Computern aus versendet. Der Angreifer installiert zunächst über das Internet auf nicht ausreichend geschützten Computern Programme[76], über die ein gleichzeitiger Angriff der verschiedenen Rechner auf einen Zielserver realisiert werden kann [vgl. Schneier 2000, 177].

Eine Möglichkeit für einen DoS-Angriff stellt das sogenannte ‚TCP SYN Flooding' [Fuhrberg 2000, 79] dar, bei dem der Zielrechner mit Paketen mit Verbindungsanfragen von nicht existenten Zielrechnern überflutet wird. Nach der Verbindungsanfrage des Clients sendet der Server ein Antwortpaket und wartet auf die Bestätigung des Verbindungsaufbaus in Form eines Antwortpakets durch den Client[77]. Verwendet der Angreifer z.B. IP-Adressen, deren Rechner nicht mehr erreichbar sind, wartet der Server vergebens und der freigehaltene Speicherplatz wird erst nach einer vorgeschriebenen Zeitspanne erneut freigegeben. Werden innerhalb dieser Zeitspanne so viele Verbindungsaufbaupakete verschickt, dass der Speicherplatz vollständig belegt ist, kann der Server keine weiteren Verbindungsanfragen entgegennehmen.

Gelingt ein DoS-Angriff beim E-Voting, auf den Wahlserver oder den Internet-Provider[78] der Wähler, besteht die Gefahr, dass Wählerstimmen nicht rechtzeitig oder gar nicht zum Wahlserver gelangen und somit auch nicht in das Wahlergebnis eingehen.

2.4.2.2 Malware

Angriffe auf einzelne Betriebssysteme können mithilfe von Malware (*Mal*icious Soft*ware*, ‚böswillige Software') durchgeführt werden. Diese Programme beinhalten unerwünschte Funktionen, die ein von der Norm abweichendes Verhalten im System herbeiführen [vgl. Schneier 2000, 143].

[76] Vgl. dazu Kapitel 2.4.2.2 zu Malware.
[77] Vgl. ausführlich zum Verbindungsaufbau [Fuhrberg 2000, 22ff.].
[78] Internet-Provider sind Anbieter für Dienstleistungen im Zusammenhang mit Zugang zum und Nutzung des Internets.

2.4.2.2.1 Computerviren

Ein sogenannter Virus ist ein nicht eigenständig lauffähiges Programm, das sich selbstständig vervielfältigt und dabei Dateien oder Systembereiche beschädigt oder modifiziert [vgl. Fuhrberg 2000, 59]. Der Virus benötigt ein Wirtsprogramm, also ein Programm von dem aus er sich in weitere Dateien, Programme und Computer kopiert. Übertragen werden Viren z.B. über Email-Anhänge oder diverse Datenträger. Generell lassen sich drei verschiedene Virentypen unterscheiden: Dateiviren, Bootsektorviren und Makroviren.

Die Dateiviren kopieren sich in den Code von Programmdateien und werden aktiv, wenn der Benutzer eine infizierte Anwendung ausführt. Durch Installation im Speicher kann der Virus weitere vom Benutzer ausgeführte Programme infizieren, indem er sich in den jeweiligen Code schreibt [vgl. Schneier 2000, 144].

Bootsektorviren dagegen kopieren sich in den Bootsektor von Festplatten oder Disketten. Bei einem Bootsektor handelt es sich um einen Speicherbereich eines Datenträgers, der einen ausführbaren Code, der beim Bootvorgang[79] geladen und ausgeführt wird, enthält. Der Virus kopiert sich in der Regel vor dem Bootsektorprogramm in den Speicher, so dass beim Hochfahren des Computers zunächst der Virus ausgeführt wird.

Makroviren verbreiten sich nicht über Programme, sondern über Dokumente und Dateien. Alle Makroviren benutzen Makro- oder Skriptsprachen, die in vielen Textverarbeitungsprogrammen, Tabellenkalkulationen oder Datenbankprogrammen verwendet werden, um Aufgaben zu automatisieren. Die Befehle der Skriptsprachen erlauben sehr weitgehende Zugriffe auf Dateien. Angriffe, die in Dokumenten versteckt werden, können daher leicht erheblichen Schaden anrichten. Zudem sind Makroviren unabhängig vom Betriebssystem und verbreiten sich schneller, da Nutzer eher Dateien als Programme austauschen [vgl. Schneier 2000, 145].

Computerviren treten in unterschiedlichen Formen auf. Während manche Viren unverändert bleiben, wechseln andere ihren Programmcode, reagieren auf Antivirenprogramme oder verschlüsseln ihren Code. Die meist destruktive Wirkung von Viren könnte den Computer des Wählers am Wahltag unbrauchbar machen und somit die Einhaltung des allgemeinen Wahlrechtsgrundsatzes gefährden. Aber auch der Wahlserver mit

[79] Der Bootvorgang bezeichnet das Hochfahren eines Computers, also die Vorgänge zwischen dem Einschalten und der Betriebsbereitschaft eines Rechners [Brockhaus 2003, 131].

den bereits eingegangen und gespeicherten Stimmen kann Opfer eines Virus' werden, der z.B. das Löschen von Voten zur Folge hat. Da ein Antivirenprogramm erst wirkt, wenn der Virus bekannt ist, stellen gezielte Angriffe am Wahltag ein besonderes Problem dar.

2.4.2.2.2 Trojanische Pferde

Trojanische Pferde (‚Trojaner') sind in ein System eingeschleuste Programmcodes, die neben den offiziellen auch verborgene, bösartige und dem Nutzer unbekannte Funktionalitäten besitzen [vgl. Fuhrberg 2000, 59]. Der wesentliche Unterschied zu Computerviren ist, dass ein Trojaner softwaretechnisch ein Computerprogramm ist und nicht die Fähigkeit besitzt, sich selbständig weiterzuverbreiten. Übertragen wird er z.B. durch einen Computervirus, einen Wurm oder per Download.

Trojanische Pferde enthalten oft Spionagefunktionen. Zum Ausspähen vertraulicher Daten wird z.B. der Tastaturpuffer überwacht und die gewonnene Information an den Angreifer weitergeleitet. Außerdem können Trojaner die Übernahme des Steuerungsprozesses des Computers vom Angreifer ermöglichen, d.h. das Öffnen oder Löschen von Dateien, die Ausführung von Programmen oder die Übernahme der Kontrolle von Maus und Tastatur [vgl. Schneier 2000, 148]. So lassen sich Wahlstimmen nicht nur aufzeichnen, sondern auch durch den Angreifer modifizieren. Ferner kann die Übermittlung ganz verhindert werden.

Ein Spezialfall eines Trojaners ist die ‚logische Bombe' [Fuhrberg 2000, 59], die als eingeschleustes Programm erst durch das Eintreten äußerer Bedingungen, z.B. Datum oder Uhrzeit, aktiviert wird. Die gezielte Aktivierungsmöglichkeit spielt im Hinblick auf den Wahltag eine besondere Rolle. So nutzen viele DDoS-Angriffe[80] im Vorfeld eine logische Bombe, um den verteilten Angriff von möglichst vielen Computern aus zu starten.

2.4.2.2.3 Würmer

Ein Computerwurm ist ein eigenständig lauffähiges Programm, das sich vor allem über Netzwerke verbreitet. Der Wurm kopiert sich dabei selbstständig auf andere Computer, um sich dort zu aktivieren. Nach erfolgreicher Infizierung eines Rechners, dient dieser als Basis für weitere Angriffe auf andere Systeme [vgl. Fuhrberg 2000, 60].

[80] Zu Denial-of-Sevice-Angriffen vgl. Kapitel 2.4.2.1.

Aufgrund seiner Eigenschaften als Programm kann ein Wurm eine spezielle Schadensroutine enthalten. Da er auf befallenen Systemen Ressourcen zur Weiterverbreitung bindet, drohen Überlastungen und Systemausfälle. Zusätzlich vermag ein Wurm Internetverbindungen zum Angreifer aufzubauen, um Informationen von lokalen Festplatten zu übermitteln. Dies gefährdet einerseits die Übermittlung der Wahlstimme durch Netz- oder Ressourcenüberlastung, andererseits die Wahrung des Wahlgeheimnisses.

2.4.2.3 Spoofing

Ein Spoofing-Angriff bezeichnet allgemein das Vortäuschen falscher Identitäten bzw. IP-Adressen [vgl. Fuhrberg 2000, 61]. Dies ist auf unterschiedliche Art möglich. Die hier dargestellten Typen stellen eine maßgebliche Bedrohung für das E-Voting dar.

Beim sogenannten IP-Spoofing werden Datenpakete mit einer falschen IP-Adresse verschickt, so dass keine Rückschlüsse auf den tatsächlichen Absender möglich sind. Die Absenderadresse eines IP-Pakets ist im sogenannten Header vermerkt. Indem der Adressteil so manipuliert wird, dass er eine andere Adresse enthält, bleibt der tatsächliche Absender unerkannt [vgl. Schneier 2000, 172]. Dies kann von Angreifern dazu genutzt werden, Sicherheitsmaßnahmen wie z.B. IP-adressbasierte Authentifizierung im Netzwerk zu umgehen. Ist eine Firewall[81] so konfiguriert, dass nur Daten bestimmter IP-Absender-Adressen (z.B. der Stimmcomputer aus Wahllokalen bzw. Wahlkiosken) angenommen werden, kann mithilfe des IP-Spoofings der wahre Absender verschleiert werden, damit die Daten durch die Firewall gelangen.

Im Fall des DNS-Spoofings greift der Angreifer in den DNS ein, also in den Internetdienst, der für die korrekte Auflösung des Hostnames verantwortlich ist. Diese Information ist nicht zentral gespeichert, sondern erfolgt durch eine Baumstruktur. Ein DNS-Server ist immer auf Informationen anderer Server angewiesen. In der Regel speichern DNS-Server die Host-Informationen, die sie von anderen DNS-Servern erhalten haben, für eine gewisse Zeit zwischen, so dass eine erneute Anfrage nach derselben Adresse schneller beantwortet werden kann. Hat ein Angreifer einen DNS-Server gehackt, hat er die Möglichkeit, die zur Verfügung gestellten Informationen, d.h. die Zuordnung einer IP-Adresse zu einem Hostname, abzuändern [vgl. Fuhrberg 2000, 63]. Der Nutzer wird nicht auf den gewünschten Server, sondern auf den Server des Angreifers geleitet. Ihm wird damit einerseits der Zugriff auf eine bestimmte Seite verweigert, gleichzeitig kön-

[81] Zur Funktionsweise einer Firewall vgl. Kapitel 2.4.3.5.1.

nen sensible Daten direkt an den Angreifer übermittelt werden, ohne dass sich der Nutzer der Gefahr überhaupt bewusst ist. Zu diesem Zweck erstellt der Angreifer eine Kopie der Originalseite, so dass der Benutzer davon ausgeht, dass eine Verbindung mit der angefragten Seite aufgebaut worden ist. Durch verschiedene Techniken können die Bereiche des Browserfensters imitiert werden, die Aufschluss über den wahren Status der Verbindung geben (z.B. Adresszeile und Statuszeile) [vgl. Fuhrberg 2000, 65]. Da der Nutzer darauf vertraut, sich auf der gewünschten Seite zu befinden, sind sensible Daten für den Angreifer leicht zugänglich, z.B. durch Abfrage eines Passworts. Darüber hinaus können gefälschte Informationen zur Verfügung gestellt werden.

Auch beim Web-Spoofing fälscht ein Angreifer einen WWW-Server, indem er durch die Gestaltung seines Servers dessen Vertrauenswürdigkeit suggeriert. Insbesondere die Wahl des Hostnames vermag in vielen Benutzern die Vorstellung zu wecken, mit einer bestimmten Institution verbunden zu sein [vgl. Schneier 2000, 161]. Internetwähler könnten davon ausgehen, die offizielle Wahlseite aufgerufen zu haben, in Wirklichkeit geben sie ihre Stimme jedoch unbemerkt auf einer vom Angreifer kontrollierten, der Wahlseite ähnelnden Seite ab. Dieser könnte die Stimme löschen, manipulieren oder ausspähen. Somit wäre die allgemeine, die gleiche und die geheime Wahl gleichermaßen bedroht.

2.4.2.4 Man-in-the-Middle-Angriff

Der sogenannte Man-in-the-Middle-Angriff ist ein Eingriff in die Kommunikation eines Netzwerkes, bei dem der Angreifer beiden Kommunikationspartnern vorspielt, der jeweils andere zu sein [vgl. Fuhrberg 2000, 94]. So kann der Angreifer z.B. mittels Spoofings die Kommunikation über seinen eigenen Rechner umleiten, ohne dass die beiden Kommunikationspartner dies merken. Beispielsweise fängt er eine Nachricht vom eigentlichen Sender ab, liest oder manipuliert sie und schickt sie an den eigentlichen Empfänger weiter, der ohne gewisse Vorsichtsmaßnahmen keine Möglichkeit hat, den Betrug festzustellen. Die in Betracht kommenden Vorsichtsmaßnahmen werden im Folgenden erörtert.

2.4.3 Technische Schutzmöglichkeiten

Die oben erläuterten Angriffsmöglichkeiten verdeutlichen die Risiken, denen eine politische Wahl im Internet ausgesetzt ist. Um die Vertraulichkeit, Integrität, Authentizität

und Verfügbarkeit der Daten zu schützen, gilt es, gezielte Gegenmaßnahmen zu ergreifen.

2.4.3.1 Kryptographie

Bei der Kryptographie handelt es sich um die Entwicklung und Bewertung von Verschlüsselungsverfahren zum Schutz geheimer Daten vor unberechtigtem Zugriff. Bei dem Verschlüsselungsprozess wird aus einer offenen Nachricht, der Klartext, durch einen bestimmten Algorithmus eine verschlüsselte Nachricht, der Chiffretext, erstellt. Die Kodierung basiert in der Regel auf einem sogenannten Schlüssel (z.B. eine geheime Zeichenkette), der vorgibt, wie die ursprünglichen Daten zu verändern sind. Zur Entschlüsselung der Daten wird ebenfalls ein Schlüssel benötigt, je nach Verfahren entweder der gleiche oder ein anderer. Da gängige Verschlüsselungsalgorithmen keine Rückschlüsse auf den verwendeten Schlüssel zulassen, kann ihre Verwendung zur Verschlüsselung ohne Einbuße der Sicherheit detailliert veröffentlicht werden [vgl. Schneier 2000, 82].

Ziel einer Verschlüsselung ist der Ausschluss der unerlaubten Entschlüsselung des Chiffretextes bzw. die Verzögerung bis zu dem Zeitpunkt, in dem der Inhalt der Nachricht irrelevant wird [vgl. Fuhrberg 2000, 81]. Prinzipiell kann jeder Schlüssel eines bekannten Algorithmus' erraten werden. Bei einem sogenannten Brute-Force-Angriff werden durch Iteration sämtliche denkbare Lösungen nacheinander durchgespielt, bis die Daten entschlüsselt sind. Eine wichtige Kennzahl eines Verschlüsselungsverfahrens ist daher die Schlüssellänge [vgl. Schneier 2000, 94]. Die maximale Dauer eines Brute-Force-Angriffs ist vom eingesetzten Algorithmus abhängig[82]. Außerdem spielen die Leistung sowie die Anzahl der eingesetzten Computer eine Rolle. Generell hat jede Aussage über die Sicherheit der Verschlüsselung nur so lange Bestand, bis ein schnellerer und leistungsstärkerer Rechner entwickelt ist. Im Allgemeinen wird davon ausgegangen, dass für sensible Daten heute eine Schlüssellänge von 1024 Bit ausreicht. Für Verfahren mit höchster Sicherheitsstufe, zu denen sicher auch die politische Internetwahl zählt, werden Verschlüsselungsverfahren ab 2048 Bit empfohlen [vgl. Forschungsgruppe Internetwahlen 2002, 18].

[82] Zur Dauer von Brute-Force-Angriffen auf verschiedene Verschlüsselungsalgorithmen vgl. z.B. [Nusser 1998, 54ff.].

Grundsätzlich kann zwischen symmetrischen und asymmetrischen Verschlüsselungsverfahren unterschieden werden. Zur sicheren Datenübertragung haben sich verschiedene Standards mit unterschiedlichen Aufgaben und Zielen etabliert[83], die oft die symmetrische und die asymmetrische Verschlüsselung kombinieren (‚Hybridverfahren'). Im Folgenden wird nicht auf die einzelnen Standards eingegangen, vielmehr werden die grundlegenden Prinzipien der Verschlüsselung erläutert.

2.4.3.1.1 Symmetrische Verschlüsselungsverfahren

Bei der symmetrischen Verschlüsselung (‚Secret-Key-Verfahren') kommt für Ver- und Entschlüsselung der gleiche Schlüssel zum Einsatz[84], so lassen sich Nachrichten relativ schnell chiffrieren und dechiffrieren[85]. Gemein haben alle symmetrischen Verschlüsselungsverfahren das Problem der Schlüsselübergabe. Sender und Empfänger müssen sich auf einen gemeinsamen Schlüssel einigen, den nur die beiden kennen. Sobald der gemeinsame Geheimschlüssel bekannt wird, ist er nutzlos.

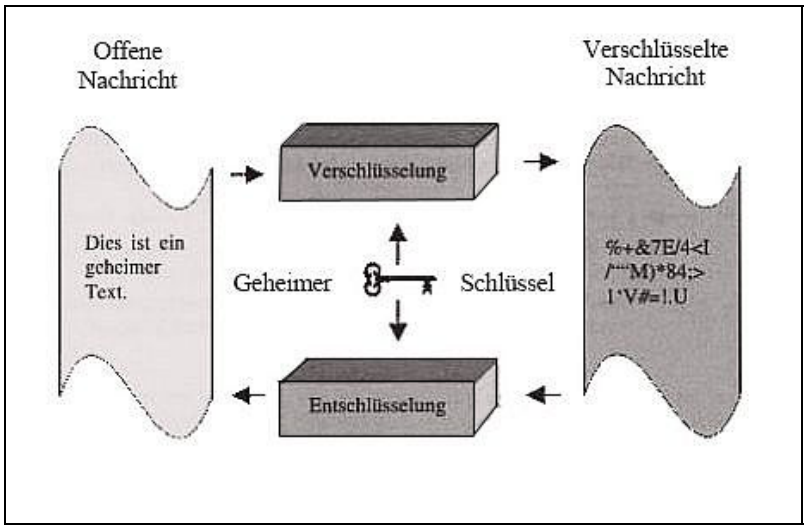

Abbildung 2: Symmetrische Verschlüsselung [Fuhrberg 2000, 84].

Ausgehend von einer paarweisen Sicherheit vervielfältigt sich das Problem der geheimen Schlüsselverteilung, da in diesem Fall die Anzahl der benötigten Schlüssel mit der Benutzeranzahl wächst. Während zwei Kommunikationspartner nur einen Schlüssel

[83] Zu den Internetstandards zählen z.B. Secure Sockets Layer (SSL) zur Absicherung der Kommunikation im WWW – Dienst zwischen Server und Client oder Pretty Good Privacy (PGP), das sich sowohl zur Datenverschlüsselung als auch zur elektronischen Signatur eignet. Vgl. ausführlich [Fuhrberg 2000, 104ff.].
[84] Zu den Standards zählen u.a. Data Encryption Standard (DES), Triple-DES und Advanced Encryption Standard (AES), vgl. ausführlich [Fuhrberg 2000, 88ff.], [Wobst 2003].
[85] Ausführlich zu verwendeten Algorithmen vgl. [Fuhrberg 2000, 85ff.].

benötigen, braucht ein 10-Personen-Netzwerk 45 Schlüssel, damit jedes Benutzerpaar sicher kommunizieren kann [vgl. Schneier 2000, 83]. Bei einer größeren Anzahl von Benutzern, von der beim E-Voting ausgegangen werden kann, scheint dieses Verfahren aufgrund der großen Menge an benötigten Schlüsseln und der unsicheren Schlüsselübermittlung unpraktikabel.

2.4.3.1.2 Asymmetrische Verschlüsselung

Bei der asymmetrischen Verschlüsselung (‚Public-Key-Verfahren') werden verschiedene Schlüssel zum Ver- und Entschlüsseln verwendet. Diese hängen zwar durch ein mathematisches Verfahren voneinander ab; eine Ableitung von einem auf den anderen darf jedoch nicht möglich sein. Um dieses Ziel zu erreichen, werden als Basis Einwegfunktionen[86] verwendet. Eine solche Funktionswertberechnung ist relativ einfach, die Umkehrung aber praktisch unmöglich [vgl. Fuhrberg 2000, 90]. Der Anwender erzeugt also zwei Schlüssel, einen öffentlichen und einen privaten. Der öffentliche Schlüssel wird dabei bekannt gegeben, der private muss unbedingt geheimgehalten werden.

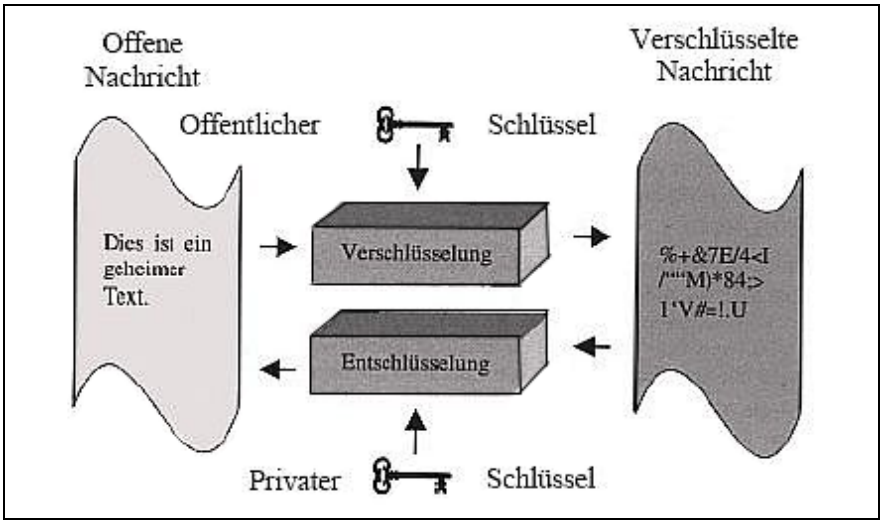

Abbildung 3: Asymmetrische Verschlüsselung [Fuhrberg 2000, 90].

Um eine Nachricht verschlüsselt zu übertragen, gibt der Absender in seinem Verschlüsselungsprogramm den öffentlichen Schlüssel des Adressaten ein. Nach der Übersendung dechiffriert der Empfänger die verschlüsselte Nachricht mit seinem privaten Schlüssel. Ohne den privaten Schlüssel des Empfängers kann der Chiffretext nicht wieder in Klartext umgewandelt werden, weshalb das Verfahren als ‚asymmetrisch' bezeichnet wird.

[86] Einwegfunktionen sind mathematische Funktionen, deren Berechnung nicht umkehrbar ist.

Die meisten asymmetrischen Verschlüsselungsalgorithmen beruhen auf mathematischen Gesetzmäßigkeiten im Zusammenhang mit Primzahlen[87]. Die Sicherheit dieser Verschlüsselungstechniken beruht auf der Schwierigkeit, eine große Zahl in ihre Primfaktoren zu zerlegen [vgl. Fuhrberg 2000, 92]. Es ist relativ einfach, geeignete große Primzahlen zu finden und zu multiplizieren und daraus den privaten und öffentlichen Schlüssel zu generieren, nicht aber umgekehrt aus dem Produkt die beiden Bestandteile herauszufinden[88] [vgl. Fuhrberg 2000, 93].

Ein Vorteil der asymmetrischen Verschlüsselung ist, dass kein geheimer Schlüsselaustausch zwischen Absender und Empfänger vonnöten ist. Sie erfordert jedoch weitaus mehr Rechenzeit als die symmetrische Verschlüsselung [vgl. Nusser 1998, 58]. Zur Verkürzung der Rechenzeit werden Hybridverfahren eingesetzt, die die Vorteile der symmetrischen und der asymmetrischen Verschlüsselung kombinieren. Hierbei sendet der Kommunikant eine mit dem öffentlichen Schlüssel seines Kommunikationspartners verschlüsselte Nachricht, die einen Sitzungsschlüssel (Session Key) gesichert überträgt. Für die weitere Kommunikation wird dann die symmetrische Verschlüsselung mithilfe des Sitzungsschlüssels genutzt. So kann eine schnelle Verschlüsselung trotz gesicherter Schlüsselübergabe gewährleistet werden.

Trotz der längeren Rechenzeit bietet die asymmetrische Verschlüsselung für das E-Voting einige Vorteile. Indem der Internetwähler sein Votum mit dem öffentlichen Schlüssel des Wahllokals verschlüsselt und an den Wahlserver schickt, kann davon ausgegangen werden, dass das Votum für Dritte unlesbar übertragen wird [vgl. Kelter et al.2001, 644]. Das Wahllokal kann anschließend die Nachricht mit seinem privaten Schlüssel wieder entschlüsseln und die Stimme speichern. Allerdings ist das Problem der Identifizierung und Authentizität des Wählers mit dem alleinigen Einsatz der asymmetrischen Verschlüsselung nicht gelöst. Zur Gewährleistung der gleichen Wahl muss sie mit weiteren Verfahren kombiniert werden.

2.4.3.1.3 Elektronische Signatur

Um die Integrität einer Wahlstimme ebenso zu gewährleisten wie die Identifizierung des Wählers, zwecks Abgleich seiner Wahlberechtigung mit dem Wählerverzeichnis, muss die asymmetrische Verschlüsselung mit der digitalen Signatur kombiniert werden.

[87] So auch der erste 1976 veröffentlichte asymmetrische Algorithmus von. Diffie/Hellmann und die RSA-Verschlüsselung, welche zu einem ‚Quasistandard im Internet' [Fuhrberg 2000, 92] geworden ist.
[88] Zu den mathematischen Details vgl. [Fuhrberg 2000, 93].

Denn ihr Ziel ist die Gewährleistung der Integrität und der Authentizität einer Nachricht [vgl. Michels 1996, 10]. Bei der digitalen Signatur handelt es sich um ein fälschungssicheres Kennzeichen, das durch Verschlüsselungsverfahren[89] erzeugt wird und mit dem die Echtheit und Herkunft digitaler Daten belegt werden kann. § 2 Absatz 1 des Gesetzes über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften[90] definiert elektronische Signaturen als

> „Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen."

Das einfachste Verfahren, mit einer Verschlüsselungsmethode eine digitale Signatur zu erzeugen, ist, mit dem privaten Schlüssel des Senders die gesamte Nachricht zu verschlüsseln und das Ergebnis an die Klartextnachricht anzuhängen. Durch dieses doppelte Versenden können zwar Manipulationen erkannt werden, es werden jedoch auch sehr große Datenmengen produziert. Daher wird das asymmetrische Verschlüsselungsverfahren mit Hashfunktionen kombiniert [vgl. Fuhrberg 2000, 98]. Die Hashfunktion[91] ist eine mathematische Einwegfunktion, die eine Prüfsumme aus der zu sendenden Nachricht bildet. Diese Prüfsumme ist quasi einmalig. Entsprechend unwahrscheinlich ist es, zu einer Prüfsumme zwei zugehörige Nachrichten zu finden [vgl. Michels 1996, 9]. Denn jedes Zeichen einer Nachricht hat Einfluss auf die Prüfsumme, d.h. bei einer Manipulation würde sich sofort auch die dazugehörige Prüfsumme verändern[92]. Der private Schlüssel des Senders wird dann nur noch auf die Prüfsumme angewendet. Das Ergebnis bildet die digitale Signatur, die dem unverschlüsselten Text angehängt wird.

Der Empfänger vollzieht den gleichen Ablauf in umgekehrter Richtung. Er entschlüsselt den Hashwert mit dem öffentlichen Schlüssel des Senders, somit ist die Identifikation des Senders sichergestellt. Als zweiten Schritt errechnet der Empfänger aus der Klartextnachricht ebenfalls den Hashwert. Entspricht dieser Wert dem vom Sender Chiffrierten, ist die Integrität der Nachricht erwiesen.

---

[89] Signierung und Verschlüsselung zum Schutz vor unerwünschter Kenntnisnahme über den Inhalt einer Nachricht sind hier zu differenzieren, auch wenn beide Verfahren auf den gleichen mathematischen Verfahren beruhen.

[90] Das Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften wird im Folgenden als SigG bezeichnet.

[91] Zu den mathematischen Hintergründen vgl. [Buchmann 2004, S. 191ff.].

[92] Bei einem Hashwert mit einer Länge von 64 Bit sind mindestens 2^{32} verschiedene Texte nötig, um eventuell einen korrekten und einen gefälschten Text mit der gleichen Prüfsumme zu erhalten [Fuhrberg 2000, 96].

2.4.3.1.4 Zertifizierungsstellen

Das beschriebene Verfahren dient der Sichtbarmachung von Manipulationen an Daten, für die Identifikation der Wähler ist es nicht ausreichend. Denn der Empfänger weiß lediglich, dass der geheime Schlüssel des Senders verwendet wurde, jedoch nichts über dessen Identität[93]. Der Signaturprüfschlüssel muss also eindeutig und rechtsverbindlich einer Person zugeordnet sein. Das SigG und die Signaturverordnung[94] regeln die technischen und organisatorischen Rahmenbedingungen, die den Einsatz der digitalen Signatur auf möglichst hohem Sicherheitsniveau gewährleisten sollen.

Das SigG unterscheidet zwischen elektronischen Signaturen, fortgeschrittenen elektronischen Signaturen, qualifizierten elektronischen Signaturen und qualifizierten elektronischen Signaturen mit Anbieter-Akkreditierung. Da erst durch eine qualifizierte elektronische Signatur oder eine qualifizierte elektronische Signatur mit Anbieter-Akkreditierung einem Internetnutzer eine reale Identität rechtsverbindlich zugeordnet werden kann[95], kommen für das E-Voting auch nur diese Ausführungen in Frage [vgl. Birkenmaier 2004, 70].

Öffentliche Schlüssel werden also nicht zwischen den Kommunikationspartnern ausgetauscht oder veröffentlicht (z.B. auf einer Website), sondern von vertrauenswürdigen Instanzen beglaubigt und in Verzeichnissen publiziert. Diese sogenannten Zertifizierungsdienstanbieter oder Trust Center bescheinigen in signaturgesetzkonformen Zertifikaten die Zusammengehörigkeit von einer natürlichen Person und dem Signaturschlüssel. Diese für die Kommunikation mit asymmetrischen Schlüsseln nötige Infrastruktur wird Public-Key-Infrastruktur (PKI) genannt. Sie ist z.B. Voraussetzung zur Vermeidung eines Man-in-the-Middle-Angriffs, da der Angreifer bei einer Schlüsselübergabe im Netz den Schlüssel des Senders abfangen und einen anderen an den Empfänger, der diesen für den tatsächlichen Schlüssel des Senders hält, schicken könnte. Der Angreifer kann jede Nachricht abfangen, entschlüsseln, lesen oder manipulieren, erneut verschlüsseln und weiterschicken ohne dass die Kommunikationspartner dies bemerken [vgl. Fuhrberg 2000, 94]. Das Problem der mangelnden Kontrolle beim Austausch der Schlüssel der Kommunikationspartner entfällt durch zertifizierte Signaturen und öffentlich zugängliche Verzeichnisse.

[93] Auf diesem Problem beruht z.B. der Man-in-the-Middle-Angriff, vgl. Kapitel 2.4.2.4.
[94] Die Signaturverordnung wird im Folgenden als SigV bezeichnet.
[95] Artikel 5 Absatz 1der Signaturrichtlinie des Europäischen Parlaments und des Rates vom 13.12.1999 normiert, dass nur von solchen Signaturen Rechtswirkungen ausgehen sollen.

Zur Zertifizierung der Signaturschlüssel bei einer qualifizierten elektronischen Signatur stellt der Zertifizierungsdienstanbieter die Identität des Antragstellers durch den Personalausweis oder Reisepass[96] fest und ordnet der Person ein generiertes Schlüsselpaar zu. Der private Schlüssel der digitalen Signatur kann auf einer Chipkarte gespeichert werden, der sogenannten Smartcard. Zum Signieren müsste der Nutzer die digitale Signatur mithilfe eines Kartenlesegeräts auslesen und sich durch eine PIN authentifizieren. Dies sichert insofern die Geheimhaltung des privaten Schlüssels, als dass die Chipkarte nur maschinell ausgelesen werden kann. Auszuschließen ist bei dieser Form der Speicherung jedoch nicht der Missbrauch durch Dritte, die sich z.B. durch Nachlässigkeit des eigentlichen Besitzers Zugang zur PIN verschaffen könnten [vgl. Will 2002, 106]. Der Empfänger der signierten Nachricht kann die Identität des Senders jederzeit online bei den Trust Centern überprüfen, die Gültigkeit des Zertifikates ist auf höchstens fünf Jahre festgesetzt[97]. Ferner muss es weitere fünf Jahre aufbewahrt werden[98], so dass Signaturen auch im Nachhinein überprüfbar sind.

Die Zertifizierung qualifizierter elektronischer Signaturen oder qualifizierter elektronischer Signaturen mit Anbieter-Akkreditierung unterliegt demselben Verfahren; es bestehen jedoch andere Anforderungen an die Zertifizierungsdienstanbieter [vgl. Hanßmann 2003, 84]. Hervorzuheben sind das Prüfverfahren nach § 15 Absatz 1 SigG als Nachweis, alle erforderlichen technischen und organisatorischen Sicherungsmaßnahmen getroffen zu haben, sowie die Aufbewahrungsdauer der Zertifikate[99]. Akkreditierte Zertifikate müssen nach dem Ablauf ihrer fünfjährigen Gültigkeit gemäß § 4 Absatz 2 SigV 30 Jahre zu einer Nachprüfung bereitgehalten werden.

Bei politischen Wahlen im Internet kommt den Zertifizierungsstellen eine besondere Bedeutung zu. Die Identifizierung des Wählers erfolgt im Vertrauen auf die Aussage eines privaten Dritten, dem Trust Center. Da in der technischen Handhabung kein Unterschied zwischen qualifizierten elektronischen Signaturen und qualifizierten elektronischen Signaturen mit Anbieter-Akkreditierung besteht, sollte beim Sicherheitsstandard das höchste Niveau angestrebt werden [vgl. Hanßmann 2003, 85]. Um Teile der Identifizierung des Wählers in private Hände abzugeben, muss gewährleistet sein, dass der Sicherheitsstandard bei den Zertifizierungsstellen regelmäßig überprüft und akkreditiert

[96] § 5 Absatz 1 Satz1 SigG i.V.m. § 3 Absatz 1 SigV.
[97] § 14 Absatz 3 Satz 1 SigV.
[98] § 4 Absatz 1 SigV.
[99] § 4 Absatz 2 SigV.

wird, da sonst eine Identitätsprüfung der Wähler durch private Dritte auch verfassungsrechtlich bedenklich wäre [vgl. Birkenmaier 2004, 73].

2.4.3.2 Anonyme Kommunikationskanäle

Der Einsatz von Kryptographie sichert also die Wahlstimmen vor dem Abhören, Mitlesen und Manipulieren durch Dritte. Ein Zusammenhang zwischen Votum und Wähler könnte dennoch hergestellt werden, da bei der Datenübertragung automatisch die IP-Adresse des benutzten Computers übermittelt wird. Die hierdurch möglichen Schlüsse auf die Herkunft der Daten könnten den geheimen Wahlrechtsgrundsatz zumindest bei einer Internetwahl vom privaten PC gefährden. Da Wahlcomputer im Wahllokal bzw. -kiosk mehreren Wählern zur Verfügung stehen, sind Rückschlüsse von der IP-Adresse des Rechners auf den einzelnen Wähler auszuschließen.

Eine Möglichkeit zur anonymen Kommunikation bieten die sogenannten MIX-Kommunikationsnetze[100], bei denen Sender und Empfänger nicht direkt miteinander kommunizieren, sondern über mindestens eine dritte Instanz, den MIX. Dies würde bedeuten, dass der Wähler sein Votum zunächst mit dem öffentlichen Schlüssel des Wahllokals verschlüsselt und an dieses adressiert. Das Ergebnis verschlüsselt er wiederum mit dem öffentlichen Schlüssel des MIX bevor er es an diese dritte Instanz verschickt. Der MIX entschlüsselt die Nachricht mit seinem privaten Schlüssel und verschickt sie an den eigentlichen Empfänger, das Wahllokal. Aus Sicherheitsgründen werden in der Regel mindestens zwei MIXe verwendet, wobei der erste nur die Ursprungs-, der zweite nur die Zieladresse kennt [vgl. Federrath et al. 2000, 150].

Um zu verhindern, dass ein Angreifer aufgrund des zeitlichen Ablaufs des Empfangens und Verschickens der Nachrichten durch den MIX Zuordnungen treffen kann, erfolgt die Versendung der empfangenen Nachrichten schubweise. Ein Schub besteht aus allen Nachrichten, die ein MIX in einem bestimmten Zeitraum empfängt. Zusätzlich werden alle ausgehenden Nachrichten auf die gleiche Länge normiert, da sonst der Angreifer den Weg der Nachricht durch das Internet allein aufgrund ihrer Bitzahl verfolgen könnte. Ein MIX puffert also die Nachrichten eines bestimmten Zeitraums, verschlüsselt sie neu und gibt sie umsortiert aus, daher der Name MIX [vgl. Kesdogan & Rattay 2005, 234].

[100] Vgl. zu den mathematischen Hintergründen ausführlich [Chaum 1981].

Wird davon ausgegangen, dass ein Angreifer das Netz kontinuierlich überwacht, ist es erforderlich, auch Nachrichten zu schicken, wenn eigentlich keine Daten übermittelt werden sollen. Diese Leernachrichten werden als ‚Dummy-Traffic' bezeichnet [vgl. Federrath et al. 2000, 151]. So ist ausgeschlossen, dass Beginn und Ende der tatsächlichen Datenübertragung vom Quellrechner zum möglichen Zielrechner beobachtet werden können.

Den MIX-Betreibern kommt bei einem solchen System eine hohe Verantwortung zu. Werden sie dieser nicht gerecht, hat das gesamte MIX-Netz seinen Sinn verfehlt. Abhilfe schaffen könnte hierbei eine Art Akkreditierung ähnlich der Zertifikationsdienstanbieter.

2.4.3.3 Blinde Signaturen

Eine weitere Möglichkeit, sowohl die Identifizierung und Authentizität des Wählers zu gewährleisten als auch die Herstellung eines Zusammenhangs zwischen Wähler und Votum auszuschließen, ist der Einsatz der blinden Signatur[101]. Im Gegensatz zur digitalen Signatur darf der Signierende hierbei nicht wissen, was er signiert. Der Inhalt einer Nachricht muss also so unkenntlich gemacht werden, dass der Signierende keine Möglichkeit hat, Rückschlüsse zu ziehen bzw. den Inhalt zu erkennen [vgl. Fuhrberg 2000, 377].

Der Geheimheitsgrundsatz erfordert die Anonymisierung der Wahlstimmen, d.h. die Entkopplung der Wähleridentität von der Stimme. Es ist somit eine anonymisierende Signatur des Stimmzettels erforderlich. Zu diesem Zweck multipliziert der Sender, im Fall des E-Votings der Wähler, seinen Stimmzettel mit einer Zufallszahl, dem Blendungsfaktor[102]. Dieser ist vom Wähler frei zu wählen und muss geheim gehalten werden. Der geblendete Stimmzettel wird vom Wähler elektronisch signiert, so dass der Wahlvorstand den Wähler zum Abgleich der Wahlberechtigung mit dem Wählerverzeichnis identifizieren kann, ohne dass der Inhalt des Votums erkannt wird. Da der ‚blinde Unterzeichner', beim E-Voting z.B. der Wahlvorstand, den vom Wähler verwendeten Blendungsfaktor nicht kennt, ist der Inhalt des Stimmzettels für ihn nicht lesbar. Der Wähler kann nach der blinden Signierung durch den Wahlvorstand den Blen-

[101] Vgl. zu den mathematischen Hintergründen ausführlich [Chaum 1982].
[102] Hierbei wird davon ausgegangen, dass die Signaturfunktion und die Multiplikation kommutativ sind.

dungsfaktor wieder herausrechnen und erhält so den vom Wahlvorstand signierten Stimmzettel. Somit ist die geheime Wahl nicht gefährdet[103].

2.4.3.4 Sicherheit des Clients

Die Maßnahmen zur sicheren Datenübertragung greifen jedoch nicht an der Schwachstelle eines E-Voting-Systems: dem Client-Rechner, also dem privaten Stimmcomputer des Wählers. Neben der nicht zu garantierenden freien und geheimen Wahl im privaten Raum gibt es erhebliche Sicherheitsbedenken, die die Internetwahl von privaten Computern „kaum begründbar" [vgl. Forschungsgruppe Internetwahlen 2002, 27] machen.

Im Wahllokal bzw. im Wahlkiosk können die Stimmcomputer mit kontrollierten Betriebssystemen und Wahlbrowsern betrieben werden. Private Computer der Wähler sind hingegen sehr viel schwieriger zu kontrollieren. Da weder ausreichender Schutz nach außen (z.B. durch eine Firewall[104]) noch die Abwesenheit von Trojanern, Viren oder sonstigen Systemanomalien auf dem Computer gewährleistet werden kann, ist nicht sichergestellt, dass die Stimme geheim und nicht manipuliert übertragen wird. Zusätzlich ist während der Stimmabgabe die Speicherung der Stimme im Arbeitsspeicher[105] oder in temporären Dateien[106] möglich. So können das Votum bzw. Information über den Wähler und seine Wahlentscheidung für Dritte zugänglich auf dem Computer zwischengespeichert werden [vgl. Europarat 2004, 57].

Eine Möglichkeit, diese Gefahren zu umgehen, wäre, ein paralleles System von einem nichtbeschreibbaren Medium (z.B. einer CD-Rom) zu starten, das nicht auf die Daten der Festplatte zugreifen muss. So ermöglicht z.B. eine sogenannte Live-CD das Starten eines Systems ohne Installation. Durch das Booten von der CD steht eine fertig eingerichtete Betriebssystem-Umgebung mit verschiedenen Anwendungen bereit, zusätzlich werden keinerlei Benutzeraktivitäten gespeichert [vgl. Brockhaus 2003, 131f.]. Beim erneuten Starten des Computers ohne CD kann das ursprüngliche Betriebssystem auf der Festplatte unverändert in Betrieb genommen werden. Für den Einsatz beim E-Voting im individuellen Bereich müsste der Wähler nur vor dem Start seines Computers

[103] Zum möglichen Einsatz in einem elektronischen Wahlverfahren vgl. Kapitel 2.4.4.
[104] Zur Funktionsweise einer Firewall vgl. Kapitel 2.4.3.5.1.
[105] Ein Arbeitsspeicher ist ein flüchtiger Speicher, in dem Programme ablaufen, d.h. die darin enthaltenen Daten sind nur so lange erhalten bis die Stromzufuhr unterbrochen oder der Computer heruntergefahren wird [Rechenberg 2000, 35].
[106] Eine temporäre Datei dient der Zwischenspeicherung von Daten während einer Arbeitssitzung, die normalerweise nach der regulären Beendigung des Programms automatisch gelöscht wird. Stürzt ein Programm ab, bleiben sie jedoch meist erhalten [Brockhaus 2003, 889].

einstellen, dass dieser als erstes das CD-Laufwerk anspricht und somit das parallele Wahlsystem startet. Es entsteht eine gesicherte Wahlumgebung, da die gegebenenfalls infizierte Festplatte des Wählers sowie installierte Hardware, z.B. ein Drucker, von dem Parallelsystem geblockt werden können.

2.4.3.5 Sicherheit des Wahlservers

Um die Sicherheit der in der Urne gespeicherten Voten zu gewährleisten, müssen Maßnahmen gegen Angriffe von außen ebenso wie gegen Angriffe von innen, d.h. gegen Hacker-Angriffe und gegen Manipulationsversuche durch zugangsberechtigte Personen (z.B. Systemadministratoren, Wahlhelfer etc.) ergriffen werden.

2.4.3.5.1 Firewalls

Schutz gegen elektronische Angriffe bietet die Implementierung einer Firewall, mit der der Datenverkehr zwischen einem internen und einem externen Netzwerk überwacht werden kann. Sie besteht aus Hard- oder Softwarekomponenten oder einer Kombination von beiden, die je nach Benutzeranforderung an die Dienste und die Sicherheit individuell konfiguriert werden können [vgl. Fuhrberg 2000, 137]. Der Einsatz unterschiedlicher Filter ermöglicht, dass nur ein bestimmtes Datenformat, ein bestimmter Absender oder eine bestimmte IP-Adresse zugelassen wird. Die Firewall sollte der einzige Zugang zum System sein, da sich nur so ihre Überwachungs- und Schutzfunktionen voll realisieren lassen. Dieser Aspekt der Leistungsfähigkeit ist beim E-Voting besonders interessant, da nur das Datenformat des Stimmzettels mit der Signatur des Wahlvorstandes durchgefiltert werden müsste [vgl. Otten 2002, 75]. Bei der Wahl von Computern aus dem Wahllokal oder einem Wahlkiosk sind zusätzlich die IP-Adressen bekannt[107], so kann ein Filter die Verbindungsanfragen dieser vorher festgelegten IP-Adressen herausfiltern und alle anderen verwerfen.

2.4.3.5.2 Maßnahmen gegen Denial-of-Service-Angriffe

Die aufgezeigten Maßnahmen für einen sicheren Datenfluss und die Datenspeicherung greifen jedoch nicht bei einem DoS-Angriff bzw. einem DDoS-Angriff[108]. Bei Gelingen eines solchen Angriffs käme das System zum Erliegen, die Durchführung einer Inter-

[107] Bei der Internetpräsenzwahl steht ein Computer nicht für einen, sondern für mehrere Wähler, somit ist die Übermittlung der IP-Adresse keine Gefahr für die geheime Wahl.
[108] Im Folgenden wird allgemein von Denial-of-Service-Angriffen gesprochen, der aber beide Arten, die einfachen und die verteilten, mit ein bezieht.

netwahl wäre unmöglich. Selbst der nur temporäre Ausfall hätte weitreichende Konsequenzen für den allgemeinen Zugang zur Wahl. Eine einheitliche Sicherheitsstrategie gegen gezielte Angriffe auf einen Server existiert momentan dennoch nicht [vgl. Birkenmaier 2004, 84].

Idealerweise sollte eine Abwehrmaßnahme wie folgt ablaufen: der Systemverantwortliche erkennt den Angriff, erarbeitet Merkmale, die den Datenstrom des Angreifers vom normalen unterscheiden, und filtert anhand dieser Merkmale die gefälschten Verbindungsanfragen heraus [vgl. Puppe & Maier 2005, 110]. In der Praxis jedoch stößt die Unterscheidung eines DoS-Angriffs von der normalen Lastspitze auf Schwierigkeiten. Selbst wenn dies gelingen sollte, ist das Herausfiltern der gefälschten Verbindungsanfragen jedenfalls wertlos, wenn die Masse der Angriffsdaten die Bandbreite des Netzanschlusses übersteigt. Der DoS-Angriff kann bei einer Internetwahl dennoch zumindest erschwert werden, indem lediglich das Datenformat des Stimmzettels zugangsberechtigt ist. Die Filterkriterien sind so eindeutig.

Die einzigen Gegenmaßnahmen basieren somit auf dem Ausbau der Bandbreite, dem schnellen Erkennen der Angriffe und dem Herausfiltern der gefälschten Anfragen [vgl. Puppe & Meier 2005, 112]. Da diese Maßnahmen keinen ausreichenden Schutz vor einem Serverzusammenbruch garantieren, ist es erforderlich, Maßnahmen zur alternativen Stimmabgabe zu ermöglichen. So ist zu gewährleisten, dass ein Internetwähler, der keinen Zugang zum System bekommt, auch auf die herkömmliche Wahl im Wahllokal in zumutbarer Entfernung zurückgreifen kann. Außerdem ist der Einsatz eines Backup-Systems ohne Medienbruch dringend zu empfehlen [vgl. Forschungsgruppe Internetwahlen 2002, 24]. Dies bedeutet, dass eine elektronische Stimmabgabe auch offline durchgeführt werden könnte. Die Wahlcomputer im Wahllokal bzw. -kiosk sollten also über ein redundantes Offline-Wahlsystem verfügen, das die abgegebenen Voten zunächst lokal speichert und zu einem späteren Zeitpunkt, also gegebenenfalls nach dem DoS-Angriff, an die Urne überträgt. Geht man davon aus, dass die Anzahl der Urnen annähernd so groß ist wie die Zahl der Wahllokale, kann bei DoS-Angriffen auf einzelne Urnen nicht von einer wahlentscheidenden Manipulation gesprochen werden [vgl. Forschungsgruppe Internetwahlen 2002, 25].

2.4.3.5.3 Technisches Audit

Um Angriffe auf ein Wahlsystem zu erkennen, ist es notwendig, das System laufend technisch zu beobachten. Systeme, mit denen ein unberechtigtes Eindringen in Netzwerke und Computersysteme erkannt und abgewehrt werden kann, werden als Intrusion Detection Systeme (IDS) bezeichnet [vgl. Schneier 2000, 187]. Ein IDS überwacht ein System permanent und schlägt Alarm, wenn bestimmte Muster im Datenverkehr auf einen Angriff schließen lassen. So werden, im Gegensatz zu einer Firewall, auch interne Angriffe miteinbezogen. Um Veränderungen im System zu bestimmen, werden automatisch Prüfsummen[109], z.B. aus Log-Dateien[110] und anderen Systemdaten, erstellt und stetig überprüft.

Die IDS nutzen hauptsächlich zwei Verfahren. Einerseits werden Filter und Signaturen eingesetzt, die spezifische Angriffsmuster enthalten. Dieses Verfahren ähnelt einem Antivirus-Programm und hat den gleichen Nachteil: es können nur bereits bekannte Angriffe erfolgreich analysiert werden. Um bisher unbekannte Angriffe zu erkennen, ist die Nutzung einer statistischen Analyse erforderlich. So kann durch vorher manuell festgesetzte Regeln oder vom System erstellte Statistiken ein abnormales Verhalten vom Regelbetrieb unterschieden werden. Die Wirksamkeit eines IDS hängt jedoch, genau wie bei der Firewall, von der Konfiguration und Aktualisierung durch den Systemadministrator ab. Diese Aufgabe darf bei einer Internetwahl nicht nur einer Person zustehen, sondern muss durch mehrere autorisierte Personen durchgeführt werden. Zusätzlich müssen Zugriffe oder Einsichten in die Protokollierungsfunktion des IDS bzw. die Protokolldaten unterbunden werden [vgl. Physikalisch-Technische Bundesanstalt 2004, 20].

2.4.3.5.4 Digitale Gewaltenteilung

Um Manipulationen durch zugangsberechtigte Personen vorzubeugen, gilt es, mehrere Instanzen mit verschiedenen Aufgabenbereichen zu schaffen. Vertrauliches Wissen muss innerhalb des Wahlprozesses gesplittet werden, damit es gegenüber Angriffen geschützt werden kann [vgl. Birkenmaier 2004, 83].

[109] Vgl. Kapitel 2.4.3.1.3 zur Berechnung des Hashwerts bei der Digitalen Signatur.
[110] Eine Log-Datei speichert automatisch ein erstelltes Protokoll über den Verlauf verschiedener Operationen.

Dies wird bei herkömmlichen Wahlen durch die Anordnung von Kompetenzen geregelt; das E-Voting erfordert diesbezüglich eine technische Umsetzung[111]. Die Überprüfung der Wähleridentität sowie seiner Wahlberechtigung, das Speichern des Votums und die Auszählung werden von unterschiedlichen Instanzen ausgeführt: den Trust-Centern, dem Wahlamt, der Urne und dem Wahlleiter. Das Wahlamt und der Wahlleiter könnten zusammen den Wahlvorstand bilden. Da zwischen den Instanzen keine direkte Verbindung bestehen darf, sollten sie nicht nur virtuell, sondern auch physisch voneinander getrennt sein [vgl. Rüß 2002, 46]. Getrennte Server und asymmetrische Verschlüsselungsverfahren stellen sicher, dass die der einzelnen Instanz zur Verfügung stehenden Daten unbedenklich sind. Nur durch Kombinierung mit dem Wissen anderer Instanzen kann das Wahlgeheimnis nicht länger gewährleistet werden. Bei Ausweitung der Berechtigungskonzepte auf Systemadministratoren und Wahlhelfer können interne Manipulationen nahezu ausgeschlossen werden [vgl. Forschungsgruppe Internetwahlen 2002, 23]. Das Sicherheitsniveau ist damit mit dem der herkömmlichen Wahl vergleichbar.

2.4.4 Skizzierung eines Wahlsystems

Um den Einsatz der erläuterten Sicherheitsmaßnahmen bei einem E-Voting-System zu verdeutlichen, soll an dieser Stelle der mögliche Ablauf einer Stimmabgabe über das Internet skizziert werden. Es wird davon ausgegangen, dass die Identifizierung der Wähler mithilfe der digitalen Signatur erfolgt. Der Wähler ist bereits Besitzer einer qualifizierten elektronischen Signatur mit Anbieter-Akkreditierung, die zur einfachen Handhabung auf einer Chipkarte gespeichert ist. Zum Auslesen der Chipkarte dient ein Kartenlesegerät; zusätzlichen Schutz vor dem Missbrauch durch Dritte bietet eine PIN.

[111] So geregelt beim ‚i-vote-System', vgl. Kapitel 3.4.1.

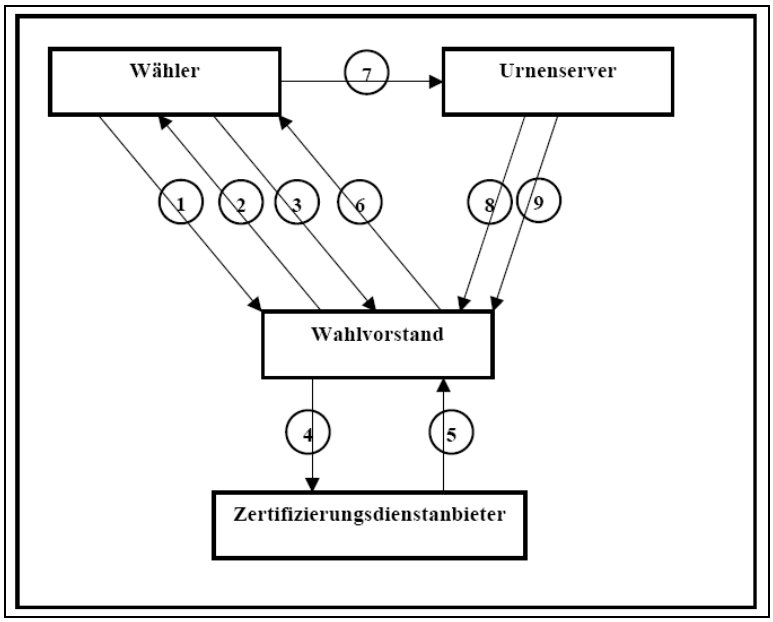

Abbildung 4: Technischer Ablauf eines Wahlsystems.

Der wahlberechtigte Internetwähler kontaktiert den für Prüfung der Wahlberechtigung zuständigen Wahlvorstand, indem er die offizielle Wahlseite aufruft. Um sicher zu gehen, dass keine nachgebildete Wahlseite eines Angreifers auf dem Bildschirm erscheint, sollte die Seite direkt über die numerische IP-Adresse aufgerufen werden. Bei einem System, das unmittelbar von einem nichtbeschreibbaren Medium gestartet wird[112], kann dies auch automatisch geschehen. Zusätzlich sollte der Wähler das Zertifikat[113] der Wahlseite manuell überprüfen. Hierfür ist eine ausreichende Kommunizierung der Zertifikatsdaten im Vorfeld der Wahl erforderlich.

Von der in Teilen geforderten Einrichtung eines zentralen Wählerregisters [vgl. Rüß 2002, 42] kann abgesehen werden, sofern die Gemeindebehörden weiterhin für jeden Wahlbezirk ein Wählerverzeichnis führen[114]. Ausgehend von der Annahme, dass die Internetwahl ähnlich der Briefwahl beantragt werden muss, ist dem Wähler bei der Zulassung des Antrags gleichzeitig die URL bzw. IP-Adresse des Heimatwahllokals mitzuteilen. Alternativ kann die Weiterleitung auch von einer zentralen Wahlseite erfolgen.

Der Wähler meldet sich also mithilfe der auf der Chipkarte gespeicherten digitalen Signatur an (1), d.h. das Kartenlesegerät liest diese aus der Chipkarte aus. Daraufhin wird

[112] Vgl. Kapitel 2.4.3.4 zur Sicherheit des Clients.
[113] Zertifizierungsstellen stellen neben Zertifikaten für digitale Signaturen auch Zertifikate für Webseiten aus. Diese können im Browser unter den Seiteninformationen abgerufen werden. Der ‚Fingerabdruck' (in Form eines Codes) einer Seite entspricht dem jeweiligen Hashwert der Seite. Da dieser einmalig ist, bietet ein Abgleich Sicherheit, dass sich der Wähler auf der offiziellen Wahlseite befindet.
[114] § 17 Satz 1 BWG.

er zu seinem zuständigen Wahllokal weitergeleitet und erhält, nach Prüfung der Wahlberechtigung durch Abgleich des Wählerverzeichnisses, die jeweiligen Stimmzettel auf dem Bildschirm (2). Nach Ausfüllen des Stimmzettels[115] wird dieser mit dem öffentlichen Schlüssel des Wahlvorstands verschlüsselt. Anschließend wird der Hashwert gebildet und der verschlüsselte Stimmzettel geblendet. Nach Signierung mit seiner elektronischen Signatur schickt der Wähler den Stimmzettel an den Wahlvorstand (3). Erfolgt die Wahl nicht von einem Wahlcomputer eines Wahllokals oder Wahlkiosks aus, sollte die IP-Adresse über einen anonymen Kommunikationskanal unkenntlich gemacht werden.

Der Wahlvorstand kann aus der Nachricht nur die elektronische Signatur des Wählers und den Hashwert der Nachricht auslesen, da der Blendungsfaktor dem Wahlvorstand unbekannt ist. Die elektronische Signatur wird mithilfe der Zertifizierungsdienstanbieter überprüft (4 und 5), die Wahlberechtigung des Wählers erneut mit dem Wahlverzeichnis abgeglichen, die Integrität der Daten durch Berechnung des Hashwerts überprüft und der Status des Wählers im Wahlverzeichnis vorläufig auf ‚hat gewählt' gesetzt. Die Signatur des Wählers wird bei einer positiven Überprüfung durch die des Wahlvorstands ersetzt. Um zu kontrollieren, ob die Stimme später auch tatsächlich zur Urne übertragen wurde, wird der Nachricht eine Seriennummer angefügt.

Der Wähler erhält die vom Wahlvorstand blind signierte Stimme (6), entfernt seinen Blendungsfaktor und verschickt die immer noch mit dem öffentlichen Schlüssel des Wahlvorstands verschlüsselte und nun auch durch den Wahlvorstand signierte Stimme, ergänzt durch die Seriennummer an den Urnenserver (7).

Die Signatur des Wahlvorstands ermöglicht dem Urnenserver bzw. seiner Firewall, ankommende Pakete zu filtern und nur Stimmen wahlberechtigter, geprüfter Wähler zu speichern. Die Seriennummer wird aus der Nachricht ausgelesen und an den Wahlvorstand geschickt (8)[116]. So kann er, ohne den Inhalt der Stimmen zu kennen, die erfolgreiche Speicherung der Voten überprüfen. Der Status des dazugehörigen Wählers wird auf ‚hat gewählt' festgesetzt.

[115] Hierbei ist eine Plausibilitätskontrolle zwecks ungültiger Stimme nötig, siehe Kapitel 2.3.3 zur freien Wahl.

[116] Es ist unbedingt erforderlich, die Seriennummer vor dem Entschlüsselungs- und Auszählungsprozess von der Stimme zu entkoppeln, da sonst die geheime Wahl durch den Wahlvorstand gefährdet würde.

Ein Zeitschloss an der Urne verhindert den Zugriff des Wahlvorstandes auf die eingegangenen und gespeicherten Stimmen vor 18.00 Uhr. Erst nach diesem Zeitpunkt können die anonymisierten Voten durch den privaten Schlüssel des Wahlvorstands entschlüsselt und anhand des Hashwerts auf ihre Integrität geprüft werden (9), bevor schließlich Zählung und Veröffentlichung des Ergebnisses erfolgen.

Trotz seiner Komplexität können bei relativ einfacher Handhabung alle nötigen Schutzmaßnahmen ergriffen werden, da das System alle Verschlüsselungstechniken, Hashwertberechnungen und Blendungsvorgänge automatisch ausgeführt.

3 Ergebnisse von E-Voting-Pilotprojekten bei politischen Wahlen und Abstimmungen

Im In- wie im Ausland haben in den letzten Jahren diverse Projekte und Initiativen zu politischen und nicht-politischen Wahlen mit Unterstützung von E-Voting-Systemen stattgefunden[117]. Die hier vorgestellten Projekte beschränken sich auf politische Wahlen und Referenden sowie die Forschung in Deutschland. Aufgrund des Umfangs dieser Arbeit und der teilweise mangelnden Dokumentation der einzelnen Projekte ist eine vollständige Darstellung nicht möglich.

3.1 Schweiz

Der schweizerische Bundestag hat 1998 mit der Initiative ‚Regieren in der Informationsgesellschaft' eine E-Government-Strategie für die nationale, kantonale und kommunale Ebene entwickelt. Neben dem ‚Guichet Virtuel'[118], dem virtuellen Behördenwegweiser für administrative Angelegenheiten, gibt es das Projekt ‚Vote Électronique'. Eine von der Bundeskanzlei initiierte Arbeitsgruppe mit Vertretern aus verschiedenen Kantonen sowie dem Bundesamt für Statistik betreut die Durchführung und Evaluation der E-Voting-Pilotprojekte, die in den Kantonen Genf, Zürich und Neuenburg durchgeführt wurden bzw. werden. Auf Basis der Ergebnisse der Evaluation erfolgt eine Entscheidung über die mögliche Einführung, jedoch voraussichtlich nicht vor 2010 [vgl. Schweizerische Bundeskanzlei 2004, 26].

Da sich einzelne Projekte in den Kantonen Zürich und Neuenburg noch in der Planungs- und Vorbereitungsphase befinden[119], konzentriert sich der folgende Teil auf den Kanton Genf, in dem bereits verschiedene rechtsgültige internetbasierte Abstimmungen durchgeführt wurden.

Durch die direktdemokratischen Elemente in der Schweizer Demokratie sind die Bürger vier bis sechs mal im Jahr aufgerufen, an Abstimmungen und Referenden teilzunehmen. Die im Jahr 1995 eingeführte Briefwahl ohne Zugangsbeschränkungen führte zu einer Steigerung der Wahlbeteiligung um 20% und wird durchschnittlich von rund 95% der Wähler in Anspruch genommen. Außerdem sind der Zugang zum und die Nutzung des Mediums Internet in der Bevölkerung weit verbreitet: 64% der Schweizer verfügen über

[117] Überblicke vgl. z.B. [Lange 2002, 129ff.]; [Will 2002, 23ff.]; [Hanßmann 2003, 40ff., 243f].
[118] Siehe http://www.ch.ch/ (Verifizierungsdatum: 16.09.2005).
[119] Siehe http://www.admin.ch/ch/d/egov/ve/projekte/projekte.html (Verifizierungsdatum: 16.09.2005).

einen Internetzugang und jeder Dritte ist täglich ‚online' [vgl. L'Etat de Genève 2005]. Die Gesetzgebung des Kantons Genf erlaubt dem Staatsrat das elektronische Wahlverfahren versuchsweise einzuführen, zusätzlich ist das Stimmregister bereits zentralisiert und technisch verfügbar; somit sind die Voraussetzungen für ein E-Voting-Pilotprojekt gegeben [vgl. Schweizerischer Bundesrat 2002, 680].

Das E-Voting-System wird größtenteils durch den Bund und den Kanton Genf finanziert und in Zusammenarbeit mit Hewlett Packet und Wisekey[120] realisiert. Die Kosten liegen bei ca. 1,3 Millionen Euro [vgl. L'Etat de Genève 2005]. Ziel dieser Zusammenarbeit ist die Unabhängigkeit von der privaten Wirtschaft und den damit verbundenen Copyrights. Der Quellcode des Systems ist für jeden Bürger offen.

Die Pilotprojekte zielen auf die Einführung des E-Votings als internetbasierte Fernwahl im individuellen Bereich; Briefwahl und Präsenzwahl bleiben in bisheriger Form bestehen. Im traditionellen Wahlverfahren erhält jeder Stimmberechtigte eine Wahlkarte per Post, die unterschrieben und mit dem Geburtsdatum versehen beim Stimmvorgang im Wahllokal abgegeben bzw. bei der Briefwahl zurückgesendet wird. Die Wahlkarten verfügen über eine Wahlkartennummer und sind jeweils nur für eine Wahl oder Abstimmung gültig. Für das E-Voting enthält diese Karte zusätzlich eine PIN, die durch ein Rubbelfeld unkenntlich gemacht ist. Sobald diese PIN zu erkennen ist, wird die Wahlkarte für Brief- und Präsenzwahl ungültig. E-Voting erfolgt, wie die Briefwahl, in einem dreiwöchigen Zeitraum vor der Präsenzwahl [vgl. Braun 2004, 46].

Zur Teilnahme am E-Voting[121] sind keine besonderen Programme auf dem Client-Rechner erforderlich. Während des Stimmvorgangs werden alle übrigen Prozesse und installierten Komponenten automatisch geblockt, nur die zur Abstimmung notwendigen Elemente sind freigegeben. Der Wähler identifiziert sich auf der Wahlseite durch seine Kartennummer, mit der ein Abgleich über den Wahlstatus des Wählers erfolgen kann. Wird der Stimmvorgang freigegeben, gibt der Wähler auf dem digitalen Stimmzettel sein Votum ab und bestätigt seine Wahl mit der PIN, seinem Geburtsdatum und der Angabe der Herkunftsgemeinde. Sind die Angaben korrekt, erhält der Wähler eine Bestätigung über die erfolgreiche Wahl mit Datum und Uhrzeit des Wahlzeitpunktes. Anders als die vorherigen Schritte kann diese Bestätigung ausgedruckt werden. Das Sys-

[120] Wisekey stellt PKI-Strukturen für sichere E-Government-Lösungen zur Verfügung.
[121] Gesamte Systembeschreibung vgl. [L'Etat de Genève 2005].

tem der Identifikation und Authentifizierung des Wählers durch PIN, Geburtsdatum und Angabe der Herkunftsgemeinde soll aus Gründen der Sicherheit ab 2006 durch digitale Signaturen unter Anwendung von Chipkarten ersetzt werden.

Die technische Infrastruktur basiert auf einem Server, der zwei Datenbanken beinhaltet, die jedoch nicht miteinander verknüpft sind: die Urne und das Wählerverzeichnis. Der Server wird durch ein mehrstufiges System gesichert. Bei der Stimmabgabe ruft der Wähler zunächst den regulären ‚Genève State Web Server' auf, der nur während einer Wahl oder Abstimmung den Zugang zum eigentlichen Wahlserver freigibt. Erst hier identifiziert sich der Wähler. Beide Server werden zusätzlich durch zwei Firewalls geschützt. Um Hacker-Angriffe zu erschweren, basieren die Server auf jeweils unterschiedlichen Technologien, da verschiedene Programmierungen selten über dieselben Fehlerquellen verfügen.

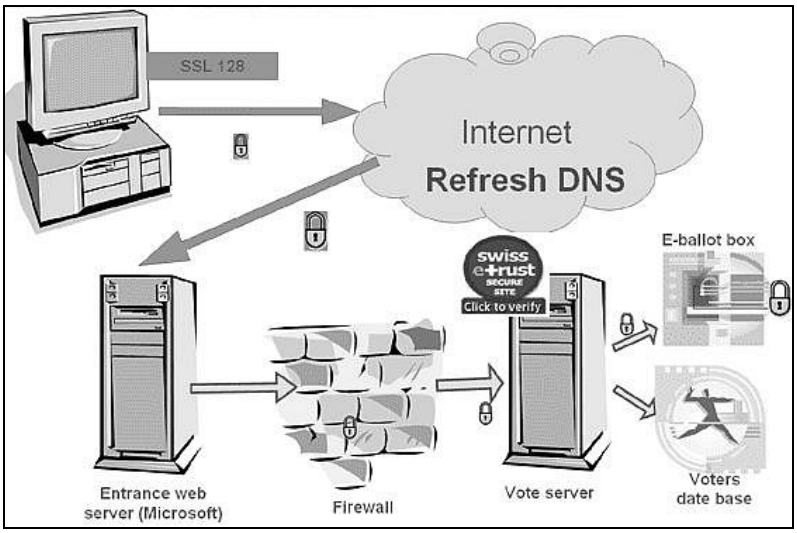

Abbildung 5: Aufbau des schweizerischen Wahlsystems [L'Etat de Genève 2005].

Um das Risiko des DNS- oder Web-Spoofing zu verringern, wird der Zwischenspeicher des DNS in höherer Frequenz als üblich erneuert. Außerdem wird ein Alarmsystem installiert, das abnormale Zustände im System oder erhöhte Verbindungsanfragen mit dem Server registriert. Ein Offline-Backup-System ist ebenfalls vorhanden.

Der gesamte Stimmvorgang basiert auf einer asymmetrischen Verschlüsselung. Zur Übermittlung der Voten wird eine SSL-Verbindung[122] erzeugt. Die abgegebenen Voten werden von der Urne mit zwei von der Datenbank verwendeten Schlüsseln verschlüsselt und gespeichert. Die zum Entschlüsseln benötigen Schlüssel sind in einem Safe ver-

[122] Secure Sockets Layer, vgl. dazu Kapitel 2.4.3.1, Fn. 83.

wahrt, die dazugehörigen Passwörter besitzt die Wahlkommission. Grund für die doppelte Verschlüsselung ist die Zusammensetzung der Wahlkommission, die aus Repräsentanten der politischen Parteien besteht. Die Mehrheitspartei bzw. Koalition erhält ein Passwort, die Opposition das andere. So hat keine Partei Zugriff auf die verschlüsselten Stimmen.

Nach verschiedenen Testläufen erfolgte im Januar 2003 die erste rechtsgültige Internet-Abstimmung in der Genfer Gemeinde Anières, bis zum April 2005 fanden sieben weitere Referenden im Kanton Genf mit der optionalen Alternative zum E-Voting statt, darunter Referenden auf Bundes-, Kantons- und Kommunalebene. Schwerwiegende sicherheitstechnische Probleme im Bereich der Organisation und Durchführung sind öffentlich nicht bekannt. Die Anzahl der Voten, die per Internet abgegeben worden sind, variieren zwischen 43, 6% der Stimmen in Anières und jeweils um die 25% in den folgenden Referenden. 80% der Wähler, die am E-Voting mindestens einmal teilgenommen haben, würden sich diese Möglichkeit auch bei politischen Wahlen wünschen [vgl. L'Etat de Genève 2005]. Diese Akzeptanz spricht für ein hohes Vertrauen in die verwendete Technik. Eine Aussage über eine höhere Wahlbeteiligung ist nur für das erste Referendum in Anières zu treffen. Hier stieg die Beteiligung um 13, 8% [vgl. Braun 2004, 47]. Für die nachfolgenden Referenden liegt kein Datenmaterial vor [vgl. L'Etat de Genève 2005].

Trotz der wenigen Auswertungsdaten scheint die zusätzliche Möglichkeit zur Stimmabgabe von den Bürgern akzeptiert und genutzt. Die direktdemokratischen Elemente der schweizerischen Demokratie lassen sich, im Vergleich zu den relativ komplexen Wahlverfahren zum deutschen Bundestag, einfacher elektronisch nachbilden, da die Stimmzettel in der Regel nur die Optionen ‚ja', ‚nein' oder ‚Enthaltung' vorsehen.

Die Geheimheit der Stimme wird rechtlich prinzipiell auch bei Referenden gewährt, jedoch sind offene politische Abstimmungen in der Schweiz ebenfalls erlaubt[123]. Außerdem ist die Briefwahl bei den Referenden, anders als bei deutschen Wahlen, keine Ausnahme zum Regelfall der Präsenzwahl im Wahllokal, sondern als fast ausschließliche Wahlform sowohl rechtlich als auch von den Wählern akzeptiert. Der Grundsatz der

[123] Die Kantone Glarus, Appenzell, Außerrhoden, Innerrhoden, Obwalden und Nidwalden praktizieren die sogenannte "Landsgemeinde", eine jährliche Versammlung bei der Beschlüsse durch Handzeichen der stimmberechtigten Bürger auf einem Platz der Stadt gefasst werden. Vgl. http://www.europarl.eu.int/enlargement/briefings/28a2_de.htm (Verifizierungsdatum: 16.09.2005).

geheimen Wahl hat also in der Praxis eher einen fakultativen als einen obligatorischen Charakter.

3.2 Großbritannien

Seit dem Frühjahr 2002 finden in Großbritannien verschiedene Pilotprojekte zur Erprobung neuer Verfahren auf kommunaler Ebene statt. Diese Projekte beziehen sich einerseits auf die Stimmabgabe mithilfe einer Touchscreen-Wahlmaschine, per Telefon, SMS und mittels Internet, im individuellen Bereich ebenso wie in Wahlkiosken und Wahllokalen. Andererseits beinhalten manche Pilotprojekte auch Verfahren zur elektronischen Stimmzählung, z.B. durch den Einsatz von Scannern [vgl. Macintosh & Xenakis 2004, 143]. Diese Projekte werden durch die Regierung gefördert und sind in die regulären Wahlen integriert, d.h. die Stimmabgabe ist rechtsgültig. Bei den Kommunalwahlen 2003 führten insgesamt 17 Gemeinden Wahlen mit der Möglichkeit zur elektronischen Stimmabgabe durch. Im Folgenden werden zwei dieser Pilotprojekte näher betrachtet, da sie eine Stimmabgabe über das Internet im individuellen Bereich sowie an öffentlich zugänglichen Stellen ermöglichten.

3.2.1 St Albans

Die Gemeinde St Albans in Hertfordshire führte im Frühjahr 2003 bereits die zweite Kommunalwahl durch, bei der u.a. die Stimmabgabe über das Internet möglich war. Das E-Voting konnte einerseits im individuellen Bereich durchgeführt werden, andererseits von Wahlkiosken an öffentlich zugänglichen Stellen. Daneben bestand die Möglichkeit, per Telefon sowie klassisch im Wahllokal und per Briefwahl zu wählen. Ziel des ‚multi-channel electronic voting' [vgl. The Electoral Commission 2003a, 2] war vor allem die Steigerung der Wahlbeteiligung und die längerfristige Reduzierung der Wahlkosten. Die Voraussetzungen für eine internetbasierte Wahl schienen gegeben; der Teil der Bevölkerung, der Zugang zum Internet hat, ist in der Gemeinde mit 86% relativ hoch.

Die technische Infrastruktur des Pilotprojekts wurde mithilfe des ‚BT Konsortiums'[124] entwickelt und umgesetzt. Teil dieses Konsortiums sind auch die Softwarehersteller Oracle und elcetion.com, wobei letzterer auf Wahlsoftware spezialisiert ist. Die Kosten liegen bei £ 1, 22 Millionen.

[124] BT ist die British Telecom, die u.a. auch Internetprovider ist.

Die Wähler hatten drei Tage vor und direkt am offiziellen Wahltag die Möglichkeit, ihre Stimme per Internet abzugeben. Zur Teilnahme am E-Voting[125] bekam jeder Wähler eine Wahlkarte, auf der sich neben dem Namen und der Adresse des Wählers, weiteren Informationen zur Wahl, den Kandidaten und zu den neuen Abstimmungsmöglichkeiten, auch eine ‚Voter Identification Number' (Voter ID) und ein Passwort befanden. Letzteres war durch ein Rubbelfeld geschützt. Die Voter ID war zusätzlich in einem Barcode enthalten, der dem Wähler ein schnelleres Registrieren in den Wahlkiosken durch Barcode-Scanner ermöglichen sollte. In den Wahlkiosken kamen reguläre Computer zum Einsatz, die mit einem Touchscreen ausgestattet waren.

Der Wähler musste die offizielle Wahlseite aufrufen und sich mithilfe des auf seiner Wahlkarte befindlichen persönlichen Barcodes, der zusätzlich durch das Passwort bestätigt wurde, identifizieren. Nach einem automatischen Abgleich mit dem elektronischen Wählerverzeichnis wählte der Wähler aus einer Liste von Kandidaten. Das Votum wurde, nach Rückfrage, abgeschickt und der Wähler erhielt als Bestätigung eine Quittungsnummer auf dem Bildschirm, die jedoch nicht ausgedruckt werden konnte. Der Status des Wählers im Wählerverzeichnis wurde auf ‚voted' gesetzt.

Sowohl die Computer im individuellen Bereich als auch in den Wahlkiosken wurden über die offizielle Wahlseite mit der E-Voting-Plattform verbunden. Die Voter ID und das jeweilige Passwort waren in der Länge genormt; beide wurden bereits bei der Eingabe durch den Nutzer mit dem privaten Schlüssel des Wahlleiters vom System verschlüsselt. Zur Übermittlung diente eine SSL-Verbindung[126] zum E-Voting-System, welches durch eine zweistufige Firewall geschützt wurde. Zusätzlich war ein IDS[127] integriert.

Das E-Voting-System bestand aus zwei separaten Datenbanken, eine für die Identität des Wählers (Wählerdatenbank) und eine zur Stimmenspeicherung (Stimmdatenbank). Die Entkopplung der Wähleridentität von der Stimme erfolgte direkt nach der erfolgreichen Weiterleitung durch die Firewall. Mithilfe der Wählerdatenbank konnte überprüft werden, wer gewählt hat, während in der Stimmdatenbank die abgegebenen Voten gespeichert wurden. Die Wahlstimmen konnten nur durch den privaten Schlüssel des Wahlleiters entschlüsselt werden. Abgesehen von unerwünschten Verbindungsanfragen

[125] Gesamte Systembeschreibung vgl. [The Electoral Commission 2003a].
[126] Secure Sockets Layer, vgl. dazu Kapitel 2.4.3.1 Fn. 83.
[127] Intrusion Detection System, vgl. dazu Kapitel 2.4.3.5.3 zum technischen Audit.

an den E-Voting-Server, die erfolgreich von der Firewall geblockt werden konnten, ist kein Wahlbetrug in Form von Manipulation oder Angriffen auf die Verfügbarkeit des Systems öffentlich bekannt geworden. Dennoch haben sich einige Probleme ergeben.

Bei der elektronischen Stimmabgabe in Wahllokalen und –kiosken wirkten sich Bedienungsprobleme negativ auf das Vertrauen der Wähler aus, da sich die Touchscreen-Computer als sehr fehleranfällig erwiesen. Neben temporären Abstürzen, die Fehlermeldungen verursachten, reagierten die Buttons auf den Touchscreens zu langsam. Zusätzlich war ein Großteil der Wähler mit dem Gebrauch der Barcode-Scanner überfordert. Dieses Problem der Nutzerunfreundlichkeit trat im individuellen Bereich nicht auf, jedoch waren hier bestimmte Systemvoraussetzungen des Wählercomputers erforderlich. Dieser Aspekt wurde im Vorfeld nicht ausreichend kommuniziert, so dass Wähler, deren Computer diese Voraussetzungen nicht erfüllten, zunächst die erforderlichen Komponenten mithilfe des Servicecenters auf ihrem Computer installieren mussten.

Das elektronische Wählerregister musste zeitweise auf ein Offline-Backup-System zurückgreifen, da die nicht ausreichende Leistung der Datenbank zur temporären Nichtverfügbarkeit führte. Die im Offline-Backup-System gespeicherten Wähler wurden im Nachhinein, aber vor der Auszählung der Stimmen, in das eigentliche Wählerregister übertragen.

Trotz aller Probleme wirkte sich das Pilotprojekt positiv auf die Wahlbeteiligung aus, die um 5% durchschnittlich auf 43, 3% gestiegen ist. 24, 4% der Stimmen wurden mithilfe des Internets im individuellen Bereich übermittelt, nur 5, 2% der Wähler nutzten Wahlkioske. Mehr als die Hälfte der Internetstimmen wurde am offiziellen Wahltag abgegeben [vgl. The Electoral Commission 2003a, 20]. Von offizieller Seite werden die durch das ‚multi-channel electronic voting' gebotenen Möglichkeiten zur Stimmabgabe besonders hervorgehoben. Die Wahlbeteiligung an der Internetwahl im individuellen Bereich spricht für die Akzeptanz der Wähler. Im Gegensatz dazu steht die sehr geringe Beteiligung an der Wahl im Wahlkiosk. Die mangelnde Benutzerfreundlichkeit der Touchscreen-Monitore erfordert Übung und Kompetenz im Umgang mit diesem Medium. Hieran scheiterten gerade ältere Wähler [vgl. The Electoral Commission 2003a, 20].

Grundsätzlich ist die Präsenzwahl zwar mit fast 40% die am häufigsten genutzte Wahlform, die unterschiedlichen Möglichkeiten zur Fernwahl, die insgesamt 55% der Stim-

men ergeben, sind dennoch bereits der Regelfall. Die Geheimheit und Freiheit ist somit bei der Mehrheit der Stimmen nicht von staatlicher Seite zu garantieren. Um die bisher hohen Kosten der ‚Multi-Channel-Wahl' zu verringern ist eine Reduzierung der Anzahl der Wahllokale geplant. Dies könnte die Tendenz zur Fernwahl noch verstärken.

Negativ zu bewerten ist die unbeständige Verfügbarkeit der unterschiedlichen Systemkomponenten. Der Ausfall der Touchscreen-Computer konnte durch die Ausweichmöglichkeit auf die herkömmliche Stimmabgabe kompensiert werden, der temporäre Ausfall des Wählerverzeichnisses stellt jedoch eine Gefahr für den Grundsatz der Gleichheit der Wahl dar. Der spätere Abgleich der Wähler mit dem Wählerverzeichnis birgt die Gefahr der Mehrfachwahl. Die offizielle Dokumentation lässt eine weitreichende Beurteilung der Systemsicherheit bezüglich des Wählerverzeichnisses aufgrund mangelnder Ausführlichkeit jedoch nicht zu.

3.2.2 Swindon

Im Frühjahr 2003 war in Swindon bereits zum zweiten Mal die Möglichkeit gegeben, bei einer Kommunalwahl auch über das Internet verbindlich abzustimmen. Hier bot das ‚multi-channel electronic voting' neben der klassischen Präsenz- und Briefwahl die Möglichkeit zur Internetwahl im individuellen Bereich sowie an Wahlkiosken, zur Stimmabgabe über das Telefon sowie über einen interaktiven, digitalen Fernseher.

Die technische Infrastruktur wurde durch das ‚Athena Konsortium' realisiert. Zu den Mitgliedern dieses Konsortiums zählen neben Anbietern für die Wahl per Telefon und Fernseher auch VoteHere Incorporated, eine Firma, die auf E-Voting-Software spezialisiert ist. Die Kosten liegen bei £ 590.000.

Die elektronischen Wahlmöglichkeiten konnten in einem Zeitraum von sieben Tagen vor dem eigentlichen Wahltag genutzt werden. Die Stimmabgabe über das Internet im individuellen Bereich oder im Wahlkiosk sowie das Wählen per interaktivem, digitalem Fernseher erfolgte über die offizielle Wahlseite im Internet[128]. Die Wahlkarte, die jeder Wähler per Post erhielt, enthielt einen zehnstelligen numerischen Zahlencode (‚Ballot Code'), der zufallsbedingt erstellt und versiegelt verschickt wurde. Zur Teilnahme an der internetbasierten Wahl gab der Wähler diesen Code auf der offiziellen Wahlseite ein. Nach automatischer Prüfung der Wahlberechtigung bzw. des Status' des Wählers

[128] Gesamte Systembeschreibung vgl. [The Electoral Commission 2003b].

durch das System, wurde der Stimmzettel angezeigt. Hierbei bestand zusätzlich die Möglichkeit, eine Erklärung der Kandidaten zur Entscheidungshilfe aufzurufen. Durch das Anklicken eines Buttons und nach erneuter Bestätigung der Stimme, wurde diese sowie die Identität des Wählers an den Wahlserver übermittelt und dort voneinander entkoppelt.

Die Übermittlung der Stimmen schütze der Aufbau einer SSL-Verbindung[129]. Alle elektronischen Abstimmungskanäle griffen auf eine zentrale E-Voting-Plattform zu, die sich aus zwei Komponenten zusammensetzte. Das sogenannte Front–End bildete die erste Komponente und war für die Zusammenführung der vier unterschiedlichen Kanäle zuständig. Um diese parallel nutzen zu können, wurde ein ‚Authentifizierungsmanager' eingesetzt, der die Datenformate der numerischen Zahlencodes zuerst vereinheitlichte. Die Daten wurden dann an die zweite Komponente, das Back-End, weitergeleitet. Hier erfolgte zunächst die Überprüfung der Gültigkeit der Zahlencodes, um so eine Mehrfachwahl durch verschiedene Kanäle zu verhindern. Die Stimme und die Identität des Wählers wurden getrennt voneinander in Tabellen gespeichert. Nach der Schließung der Wahllokale erfolgte die Versendung der elektronisch gespeicherten Stimmen per Email, verschlüsselt durch PGP[130], an den Wahlvorstand.

Der Wahlvorstand hatte während des gesamten E-Voting-Zeitraums Zugriff auf eine Wahlstatistik, die in Echtzeit über die abgegebenen Stimmen auf den verschiedenen Kanälen erzeugt wurde. Gleichzeitig erfolgte die Erstellung eines Registers über die elektronischen und postalischen Wähler. Die aus der Statistik ermittelte Anzahl der abgegebenen Stimmen und die Anzahl der Wähler aus dem Register wurden nach Ablauf der Wahl miteinander abgeglichen, um eventuelle Unstimmigkeiten zu prüfen. Das Register diente am eigentlichen Wahltag, an dem nur noch Präsenzwahl möglich war, ebenfalls der Kontrolle der Präsenzwähler. Da alle Fernwähler in dem Register vermerkt waren, konnte eine Mehrfachwahl nahezu ausgeschlossen werden.

Die Durchführung des ‚multi-channel electronic voting' ist von offizieller Seite als Erfolg gewertet worden. Es wurden keine Angriffe oder Manipulationsversuche bekannt. Ein Viertel aller abgegebenen Stimmen ist auf elektronischem Weg eingegangen, davon fast 70% über das Internet. Während der Wahlzeit hatten alle Wähler die Möglichkeit,

[129] Secure Socket Layer, vgl. Kapitel 2.4.3.1, Fn. 83.
[130] Pretty Good Privacy, vgl. Kapitel 2.4.3.1, Fn. 83.

bei Problemen Hilfe und Unterstützung per Telefon zu erhalten. Diese Möglichkeit nutzten jedoch nur 0, 7% der Internetwähler[131]. In einer freiwilligen Befragung nach der Stimmabgabe gaben fast 95% der Internetwähler an, die Stimmabgabe sei ‚very easy'; 60% hatten ebenso großes Vertrauen in das E-Voting-System wie in die herkömmliche Wahl.

Trotz dieser positiven Resonanz der Internetwähler ist die Wahlbeteiligung leicht um 2% zurückgegangen. Eine geringe Wahlbeteiligung lässt sich jedoch bei allen Kommunalwahlen 2003 in Großbritannien feststellen. Allein das Angebot neuer Möglichkeiten zur Stimmabgabe führte in diesem Fall also nicht zu einer höheren Wahlbeteiligung.

Obwohl keine Manipulationen oder Angriffe auf die Verfügbarkeit bekannt sind, lassen sich die sicherheitstechnischen Vorkehrungen als nicht ausreichend bewerten. Die Authentifizierung der Wähler erfolgt nur durch den numerischen Zahlencode. Durch einen Brute-Force-Angriff[132] mit leistungsstarken Rechnern kann dies ein Risiko für die einfache Stimmabgabe und damit für die gleiche Wahl darstellen. In der offiziellen Dokumentation sind einige wichtige Aspekte unzureichend erläutert, z.B. der genaue Zeitpunkt der Entkopplung von Wähleridentität und Stimme. Ebenso ist fraglich, ob ein Zusammenhang zwischen Wähler und numerischem Zugangscode durch Speicherung der Angaben im Wählerregister erkenntlich und überprüfbar ist. Dies würde die geheime Wahl gefährden, da Zugangscode und Stimme während des Übermittlungsvorgangs nicht getrennt sind. Zudem ist der Grundsatz der freien Wahl in diesem E-Voting-System durch die Möglichkeit, beim Stimmvorgang Erklärungen einzelner Kandidaten aufzurufen, nicht vollständig gewahrt, da die unbeeinflusste Stimmabgabe nicht gewährleistet werden kann.

3.3 Estland

Im Herbst 2005 wird in Estland die Stimmabgabe über das Internet bei Kommunalwahlen zum ersten Mal rechtsverbindlich zugelassen. Dabei handelt es sich ausschließlich um die internetbasierte Fernwahl im individuellen Bereich. Die herkömmlichen Wahlformen der Präsenzwahl im Wahllokal und die Briefwahl bleiben bestehen. Die Rechtsgrundlage für Internetwahlen beschränkt sich jedoch nicht auf die kommunale Ebene,

[131] Im Gegensatz dazu machten 20% der Wähler, die per Telefon abstimmten, Gebrauch von der Telefonhotline.
[132] Zum Brute-Force-Angriff vgl. Kapitel 2.4.3.1.

sondern ist auch bei nationalen und europäischen Wahlen sowie bei Referenden gegeben [vgl. The National Election Committee 2004, 4].

Seit Mitte der neunziger Jahre initiiert die estnische Regierung Programme zur Förderung der Verbreitung und Nutzung der neuen Informations- und Kommunikationstechnologien in der Bevölkerung[133] [vgl. Steiner 2005, 1]. Neben einem Bürgerportal[134], in dem u.a. Gesetzesvorlagen diskutiert werden können, werden z.B. Parlamentssitzungen online live übertragen [vgl. Narusberg 2004, 1]. Im Dezember 2000 trat in Estland das Gesetz zur digitalen Signatur in Kraft; seit 2002 ist diese digitale Signatur sowie ein digitales Signaturzertifikat gemäß des estnischen Signaturgesetzes in jedem Personalausweis integriert, dessen Besitz seit Januar 2002 Pflicht für alle estnischen Staatsbürger und permanenten Bewohner über 15 Jahren ist. Neben den Eigenschaften eines gängigen Ausweispapiers soll die estnische ID-Card umfassend für rechtlich bindende Online-Transaktionen eingesetzt werden und ist Voraussetzung zur Teilnahme am E-Voting. Aktuell sind knapp über 800.000 Esten Inhaber eines solchen Ausweises[135]; diese Zahl entspricht beinahe den bei Kommunalwahlen Wahlberechtigten [vgl. Maaten 2004, 85].

Kennzeichnend für das estnische E-Voting-System ist das Prinzip der mehrfachen Stimmabgabe (‚re-vote'), wobei jede erneute die vorherige ungültig werden lässt. Um Wahlbeeinflussung oder Stimmenkauf zu verhindern, kann der Wähler seine zuerst abgegebene Stimme einerseits durch eine wiederholte elektronische Wahl korrigieren, andererseits auch am Wahltag im Wahllokal eine erneute Stimme abgeben. Die Wahl über das Internet findet vom sechsten bis zum vierten Tag vor dem eigentlichen Wahltag statt. Die Präsenzwahl im Wahllokal gilt grundsätzlich als letzte Entscheidung [vgl. Maaten 2004, 86].

Der Wähler ruft die offizielle Wahlseite des National Electoral Committee[136] auf und identifiziert sich mithilfe seiner auf dem digitalen Personalausweis befindlichen elektronischen Signatur, die von einem Kartenlesegerät[137] ausgelesen wird. In einem elekt-

[133] Neben Schulungen und Kursen wurden öffentlich zugängliche, kostenfreie Internetzugänge in öffentlichen Gebäuden, Jugendherbergen, Hotels etc. bereitgestellt. Vgl. [Steiner 2005].
[134] Siehe http://tom.riik.ee/ (Verifizierungsdatum: 16.09.2005).
[135] Statistiken über die Anzahl der Karteninhaber siehe http://www.id.ee/pages.php/03030102 (Verifizierungsdatum: 16.09.2005).
[136] Systembeschreibung vgl. [The National Election Committee 2004].
[137] Das ID-Karten-Starterkit muss jeder Bürger selbst finanzieren. Die Kosten liegen bei ca. 20 € und beinhalten neben dem Kartenlesegerät auch die erforderliche Software [Narusberg 2004].

ronischen Wählerverzeichnis ist der Heimatwahlkreis jedes Wählers neben seiner Identifikationsnummer vermerkt. Nach der erfolgreichen Identifikation kann so der Stimmzettel des jeweiligen Wahlkreises dem Wähler in digitaler Form vorgelegt werden. Der Wähler kennzeichnet den Stimmzettel, bestätigt seine Wahl und signiert das automatisch verschlüsselte Votum. Nach erfolgreichem Versenden erhält der Wähler eine Bestätigung seiner Wahl auf dem Bildschirm. Der Status des Wählers im elektronischen Wählerverzeichnis wird auf ‚elektronisch gewählt' gesetzt.

Das Konzept des E-Voting-Systems basiert auf der ‚Briefumschlag-Methode' (‚envelope method'). Diese Methode veranschaulicht die Vorgänge der Internetwahl durch ein ‚Ineinanderstecken' mehrerer virtueller Briefumschläge. Der Wähler verschlüsselt sein Votum (verschlüsselte Stimme = innerer Briefumschlag) mit dem öffentlichen Schlüssel des Wahlsystems und signiert das Ergebnis (signierte Daten = äußerer Briefumschlag). Diese Daten werden an das zentrale Wahlsystem geschickt, das aus mehreren Komponenten besteht.

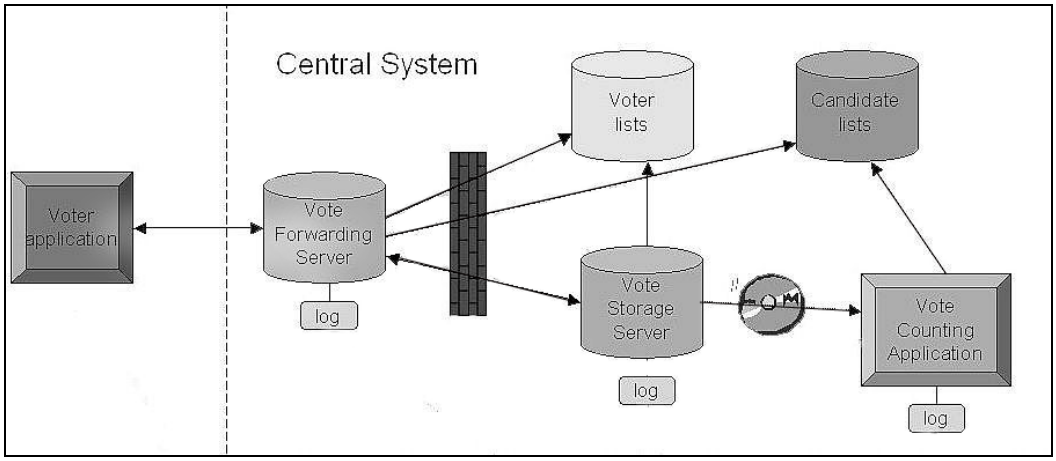

Abbildung 6: Aufbau des estnischen Wahlsystems [The National Election Committee 2004, 10].

Der Vote Forwarding Server (VFS) ist die einzige über das Internet direkt zugängliche Komponente des Systems, mit der der Wähler während des Wahlvorgangs kommuniziert. Anhand der digitalen Signatur erfragt der VFS den Heimatwahlkreis und die dazugehörige Kandidatenliste aus der VoterList- bzw. der CandidateList-Datenbank. Zusätzlich wird mithilfe einer Anfrage an den Vote Storage Server (VSS) kontrolliert, ob der Wähler bereits gewählt hat. Ist dies der Fall, wird er darauf hingewiesen. Die verschlüsselte, signierte Stimme wird vom VFS an den VSS weitergeleitet. Der VSS hat Zugriff auf den Validity Confirmation Server (VCS), der die Gültigkeit der digitalen Signaturen anhand von Zertifikaten überprüft. Nach einer positiven Prüfung wird die

Stimme mit der Signatur (der äußere Briefumschlag) im VSS sowie der Wähler in einer E-Voter-Liste gespeichert. Mithilfe dieser Liste kann geprüft werden, ob der Wähler bereits zuvor elektronisch gewählt hat, gegebenenfalls ersetzt die zuletzt eingegangene Stimme die vorherige. Aufgrund dieser Möglichkeit zum re-vote kann die Entkopplung der Wähleridentität von seiner Stimme erst nach Schließung der Wahllokale erfolgen, da jedem Wähler die Präsenzwahl am eigentlichen Wahltag offen steht und sonst die einfache Stimmabgabe nicht gewährleistet werden könnte.

Nach Schließung der Wahllokale wird die E-Voter-Liste mit den Wählerlisten der Präsenz- und der Briefwahl abgeglichen, bei einer Mehrfachwahl erfolgt die Löschung der elektronischen Stimme. Die gültigen elektronischen Stimmen werden nach ihren Wahlkreisen sortiert, die der VFS anhand der digitalen Signatur durch Abfrage der VoterList-Datenbank ermitteln kann. Um die Wahlstimmen zu anonymisieren, wird die elektronische Signatur (der äußere Briefumschlag) entfernt und nur das mit dem öffentlichen Schlüssel des Wahlsystems verschlüsselte Votum (innerer Briefumschlag) gespeichert. Die letzte Komponente des E-Voting-Systems bildet die Vote Counting Application (VCA), die für das Entschlüsseln und Zählen der Stimmen zuständig ist. Da dies offline geschieht, ist für die Übertragung der gültigen, verschlüsselten Stimmen ein externes Speichermedium erforderlich. In der VCA werden die Voten mit dem privaten Schlüssel des Wahlsystems entschlüsselt und gezählt. Der private Schlüssel des Wahlsystems wird von einer Gruppe ‚key manager' aufbewahrt und ist durch eine PIN geschützt. Das Wissen über diese PIN ist zwischen den ‚key managern' aufgeteilt, so dass keine Einzelperson Zugang zum privaten Schlüssel hat.

Um das E-Voting-System technisch vor Angriffen von außen zu schützen, werden mehrstufige, kombinierte Firewalls eingesetzt. Zusätzlich schützt ein Audit-System[138] die Integrität der Stimmen. Als Kontrollfunktion werden bei jeder Komponente des Wahlsystems Log-Dateien[139] angelegt, jeweils eine für die gültigen und eine für die ungültigen Stimmen. In den Log-Dateien wird nur der automatisch generierte Hashwert des Votums gespeichert. Durch einen späteren Abgleich kann die Integrität der Stimme nachgewiesen werden. Die Authentifizierung der Wähler ist durch die Public-Key-Infrastruktur der digitalen Ausweispapiere gesichert.

[138] Vgl. Kapitel 2.4.3.5.3 zum technischen Audit.
[139] Eine Log-Datei speichert automatisch ein erstelltes Protokoll über den Verlauf verschiedener Operationen.

Im Januar 2005 erfolgte das erste Pilotprojekt im Rahmen eines lokalen Referendums in Talinn. Eine vollständige Dokumentation ist öffentlich nicht verfügbar. Trotz der mangelnden Erprobung wird das System im Oktober bei den kommunalen Wahlen eingesetzt. Falls es zu Systemausfällen oder erkennbaren Manipulationen kommt, ist durch die Möglichkeit zum ‚re-vote' die Präsenzwahl am eigentlichen Wahltag und somit der Grundsatz der allgemeinen Wahl gewahrt. Es ist jedoch fraglich, ob sich ein Abbruch der Internetwahl bzw. ein Ausweichen auf die herkömmliche Präsenzwahl nicht negativ auf die Wahlbeteiligung und auf das Vertrauen der Bürger in die Regierung auswirken könnte. Zusätzlich widerspricht die in dem estnischen E-Voting-System gültige Möglichkeit zum ‚re-vote' dem Grundsatz der gleichen Wahl, da Präsenz- und Briefwähler nicht die Möglichkeit haben, ihre Stimme zu revidieren.

Möglichkeiten zu Angriffen ergeben sich vor allem während der Speicherung der Stimmen. Zwar sind Manipulationsversuche durch den gespeicherten Hashwert überprüfbar, die späte Entkopplung von Wähleridentität und Stimme könnte den Grundsatz der geheimen Wahl jedoch gefährden. Das externe Speichermedium zur Übermittlung der gültigen Stimmen von dem VSS zur VCA stellt durch möglichen Verlust oder Diebstahl einen weiteren Angriffspunkt dar. Es ist fraglich, warum auf diese Methode zurückgegriffen wird, anstatt die gespeicherten Stimmen über eine gesicherte Verbindung zur VCA zu übertragen.

3.4 Initiativen und Forschung in Deutschland

3.4.1 Forschungsgruppe Internetwahlen/ Wählen in elektronischen Netzwerken (W.I.E.N.)

In Deutschland gründete die Universität Osnabrück anlässlich der Bundestagswahl 1998 den ‚Wahlkreis 329'[140] . Das Projekt dient der virtuellen Simulation der Bundestagswahl im Internet. Die Teilnehmer können auf der Internetseite mithilfe einer auf Anmeldung erteilten TAN ihre Stimme sowie einen Tipp über den Ausgang der Wahl abgeben. Während der zweiwöchigen Laufzeit der Plattform 1998 besuchten knapp 300.000 Internetnutzer den virtuellen Wahlkreis, darunter 16.975 Wahlteilnehmer. Die aus den Tipps ermittelte Wahlprognose wich lediglich um 1, 1% vom tatsächlichen Wahlergebnis ab [vgl. Otten 1998, 27]. Aus dem Projekt entstand die Forschungsgruppe

[140] Seit der Bundestagswahl 2002 läuft das Projekt unter dem Namen ‚Wahlkreis 300'. Vgl. www.wahlkreis300.net (Verifizierungsdatum: 16.09.2005).

Internetwahlen an der Universität Osnabrück, deren Ziel es ist, ein verfügbares Online-Wahlverfahren zu entwickeln und unter Tests zu optimieren. Die Tests beziehen sich jedoch bisher ausschließlich auf nicht-politische bzw. nicht-parlamentarische Wahlen. Ein Zusammenschluss der Forschungsgruppe Internetwahlen, des Landesbetriebes für Datenverarbeitung und Statistik (LDS) Brandenburg und der T-Systems CSM Darmstadt bildet unter Förderung des Bundesministeriums für Wirtschaft und Arbeit das Folgeprojekt ‚Wählen in elektronischen Netzwerken' (W.I.E.N.)[141].

Die bisher durchgeführten Pilotprojekte[142] basieren auf dem von der Forschungsgruppe Internetwahlen entwickelten System ‚i-vote'. Anstatt einer ausführlichen Systembeschreibung sind allein ein Kurzbericht der Forschungsgruppe Internetwahlen sowie die Abschlussberichte der mit ‚i-vote' durchgeführten Testwahlen, die in der Literatur bereits ausführlich dargestellt werden[143], öffentlich zugänglich. Im Folgenden werden aus diesen Quellen der Ablauf einer mit ‚i-vote' durchgeführten Wahl beschrieben sowie die aus den Testwahlen resultierenden Probleme und Erkenntnisse erörtert.

Grundlegend für das ‚i-vote'-System ist das Prinzip der ‚digitalen Gewaltenteilung' in Form eines Drei-Instanzen-Konzeptes. Diese Teilung erfolgt durch Verwendung zweier Server, des Wahlamt- (‚Validator') und des Urnenservers (‚Psephor'). Der Validator verwaltet die Wählerliste und autorisiert den Wähler zur Wahl, während der Psephor über die Urnen der einzelnen Wahlbezirke verfügt. Ein von den Servern physisch getrennter Computer übernimmt als ‚Wahlleiter' die spätere Stimmenauszählung. Die Administratoren der Server und des ‚Wahlleiters', die zusammen den Wahlvorstand bilden, sind nicht nur rechtlich und personell, sondern auch physisch voneinander getrennt und stehen dabei unter öffentlicher Kontrolle [vgl. Otten 2002, 79]. Das Drei-Instanzen-Konzept soll für jeden Wahlkreis gelten, d.h. es gibt kein zentrales Wählerverzeichnis.

Obwohl bei der Mehrheit der Testwahlen eine internetbasierte Fernwahl im individuellen Bereich möglich war, ist für die Forschungsgruppe diese Form des E-Votings aufgrund von Sicherheitsbedenken und der Gefahr für die Freiheit der Wahl „kaum begründbar" [Forschungsgruppe Internetwahlen 2002, 27]. In Wahllokalen bzw. Wahlkiosken kommen Computer zum Einsatz, auf denen ausschließlich ein generisches Wahl-

[141] Vgl. http://www.forschungsprojekt-wien.de/ (Verifizierungsdatum: 16.09.2005).
[142] Vgl. http://www.internetwahlen.de/ unter i-vote Projekte (Verifizierungsdatum: 16.09.2005).
[143] Vgl. z.B. [Lange 2002], [Will 2002], [Hanßmann 2003].

system installiert ist. Unabhängig von seinem Heimatwahlkreis begibt sich der Internetwähler in ein beliebiges Wahllokal und identifiziert und authentifiziert sich durch eine PIN-geschützte Chipkarte, auf der eine digitale Signatur gespeichert ist. Der Wahlamtserver leitet den Wähler aufgrund seiner Identität zum entsprechenden Stimmzettel seines Heimatwahlkreises. Nach einer zu bestätigenden Rückfrage zur Wahlentscheidung wird das Votum mit dem öffentlichen Schlüssel des Wahlleiters verschlüsselt, geblendet, mit der digitalen Signatur des Wählers signiert und zwecks einer blinden Signatur[144] an den Validator geschickt. Dieser überprüft die Wahlberechtigung, signiert das Votum und setzt den Status des Wählers auf ‚gewählt'. Der Wähler wiederum entblendet die vom Validator blind signierte Nachricht, entfernt zwecks Anonymisierung der Stimme seine persönliche digitale Signatur und schickt das verschlüsselte Votum an den für sein Wahllokal zuständigen Psephor. Nach Beendigung der Wahl schickt der Psephor die verschlüsselten Voten an den ‚Wahlleiter', der diese entschlüsselt und auszählt [vgl. Otten 2002, 82; vgl. Otten & Küntzler 2002].

Die Identifizierung des Wählers erfolgt durch eine zertifizierte digitale Signatur, die aber vor der Stimmenspeicherung wieder vom Votum entkoppelt wird. Beide Informationen werden nicht ungeschützt zusammen kommuniziert. Der Psephor erhält also keine Informationen über die Identität des Wählers, sondern nur durch die Signatur des jeweiligen Wahlvorstands anonymisierte Voten. Entschlüsselt werden können die Stimmen lediglich durch den privaten Schlüssel des Wahlvorstands, auf den die Urnenadministratoren keinen Zugriff haben. Zusätzlich schützt ein Zeitschloss die Stimmen im Psephor bis zum offiziellen Wahlende [vgl. Forschungsgruppe Internetwahlen 2002, 20ff.]. Das Serversystem des Psephors beinhaltet ein Backup-System, das permanent eine verschlüsselte Spiegelung der Urne vornimmt. Dies ermöglicht eine Verifizierung der Wahl durch Nachkontrolle. Zusätzlich sollen in den Wahllokalen Offline-Systeme bereitstehen, die bei einem Ausfall des Systems eine Stimmabgabe ohne Medienbruch ermöglichen [vgl. Otten 2002, 80].

Die Nutzung der speziellen Software des ‚i-vote'-Systems sowie die Identifizierung des Wählers per Chipkarte haben sich in den Testwahlen als schwierig erwiesen [vgl. Lange 2002, 134]. Da bei allen Wahlen auch eine internetbasierte Fernwahl im individuellen Bereich möglich war, musste zunächst die Wahl- und Kartenlesegerätsoftware installiert

[144] Zum Verfahren der blinden Signatur vgl. Kapitel 2.4.3.3.

werden. Bei der „ersten rechtskräftigen Parlamentswahl über das Internet“ [Forschungsgruppe Internetwahlen 2002, 5] zum Studierendenparlament der Universität Osnabrück erzeugte dies Probleme: 30% der Internetwähler im individuellen Bereich scheiterten [vgl. Forschungsgruppe Internetwahlen 2000, 39]. Auch bei der Jugendgemeinderatswahl in Esslingen 2001 erschwerten Installationsprobleme die Teilnahme [vgl. Steinbeis-Transferzentrum Mediakomm 2001, 26].

Die zur Authentifizierung des Wählers benötigten Chipkarten führten in vielen Testwahlen zu Problemen. Zum einen waren digitale Signaturen trotz erfolgreicher Installation der Kartenlesegeräte nicht lesbar, zum anderen erwies sich die Handhabung der Chipkarten als fehleranfällig. Bei den Personalratswahlen im LDS Brandenburg im Mai 2002 wurde durch falsche Bedienung die Chipkarte in mehreren Fällen ungültig [vgl. LDS 2002, 34]. Bei den Wahlen zum Betriebsrat bei T-Systems CSM im Mai 2002 konnte auf firmeninterne Chipkarten zurückgegriffen werden, so dass aufgrund der Übung keine Probleme in der Handhabung entstanden. Im Verlauf der Wahl an der Universität Osnabrück und im LDS Brandenburg kam es zusätzlich zu temporären Netzausfällen und damit zu einer Nicht-Verfügbarkeit des Wahlservers [vgl. Lange 2002, 132 ff.]. Bei Letzterem wurde bei der Stimmzählung eine Differenz zwischen den in der Urne gespeicherten Stimmen und der im online geführten Wählerverzeichnis als ‚online gewählt’ vermerkten Wähler registriert. Die Fehlerursache ist unklar [vgl. Hanßmann 2003, 59].

3.4.2 Weitere Pilotprojekte

Außer den mit dem ‚i-vote’-System realisierten Testwahlen wurden in Deutschland verschiedene andere Pilotprojekte durchgeführt. Neben den Jugendgemeinderatswahlen in Fellbach (Baden-Württemberg) im Juni 2001 und in Bobenheim-Roxheim (Rheinland-Pfalz) im November 2001 fand auch die erste Internettestwahl im Rahmen einer politischen Wahl auf Kreisebene im Landkreis Marburg-Biedenkopf (Hessen) im September 2001 statt. Interessant ist die Tatsache, dass bei diesen Projekten die Identifikation des Wählers nicht durch digitale Signaturen erfolgte, sondern mithilfe des PIN/TAN-Verfahrens. In Fellbach führte dies jedoch zu Manipulation und Wahlbetrug, indem TANs entwendet und zur mehrfachen Stimmabgabe missbraucht wurden [vgl. Stadt Fellbach 2001, 11].

In Marburg-Biedenkopf konnten alle Briefwähler parallel zur rechtsverbindlichen Wahl ihre Stimme unverbindlich im Internet von jedem Computer im individuellen Bereich abgeben. Nach erfolgreicher Identifizierung durch die vorher beantragten PIN und TAN sowie der Überprüfung der Wahlberechtigung konnte der Wähler seine Stimme auf einem digitalen Stimmzettel abgeben. Auf einer weiteren Seite erfolgte durch Anklicken eines Buttons eine Versicherung an Eides Statt. Die Datenübertragung sicherte eine SSL-Verbindung[145]. Die abgegebenen Stimmen wurden zwar verschlüsselt, jedoch mit der PIN und TAN des Wählers in der Urne gespeichert [vgl. Projekt ESI 2001, 6]. Dies könnte zu einer Gefährdung des Wahlgeheimnisses führen, da die Daten erst vom Wahlleiter entschlüsselt wurden, bevor eine Entkopplung der personenbezogenen Daten von der Stimme erfolgte.

Insgesamt wurde die Testwahl im Landkreis Marburg-Biedenkopf offiziell als Erfolg gewertet, die Identifizierung durch das PIN/TAN-Verfahren aber gerade bezüglich der Sicherheit (Missbrauch oder Entwendung durch Dritte) und der fehlenden rechtlichen Grundlage zur Versicherung an Eides Statt als verbesserungswürdig bezeichnet. Eine auf einer Chipkarte gespeicherte digitale Signatur wird hier als Lösungsmöglichkeit gesehen [vgl. Projekt ESI 2001, 11ff].

[145] Secure Sockets Layer, vgl. dazu Kapitel 2.4.3.1, Fn. 83.

4 Auswirkungen von Internetwahlen – erste Erfahrungen und Annahmen

Neben den genannten, verfassungsrechtlich normierten Wahlrechtsgrundsätzen existieren weitere, ungeschriebene' [vgl. BVerfGE 2, 380(403)]. Darunter fällt z.B. die weitgehende Kostenfreiheit für den Wähler, die Kontrollfunktion der Öffentlichkeit während der Wahl sowie die Verständlichkeit und Nachvollziehbarkeit des gesamten Wahlablaufs [vgl. Karpen 2005, 31]. Bei einer technischen Erweiterung des Wahlverfahrens sollten auch die möglichen Auswirkungen auf diese Aspekte betrachtet werden, da sie eventuell Einfluss auf die Wahlbeteiligung sowie das Wählervertrauen haben könnten.

4.1 Finanzieller Aufwand

Gemäß § 50 Absatz 1 BWG „erstattet der Bund den Ländern zugleich für ihre Gemeinden die durch die Wahl veranlassten notwendigen Ausgaben." Diese beinhalten die Kosten für die Versendung von Wahlbenachrichtigungen und der Briefwahlunterlagen, die Entlohnung (‚Erfrischungsgelder') der Wahlhelfer, Druck- und Papierkosten für Stimmzettel und Briefumschläge, Kosten für öffentliche Bekanntmachungen sowie für die Anmietung zusätzlicher Wahlräume [vgl. Schreiber 2002, 679]. Die Kosten für die Versendung der Wahlbenachrichtigungen und der Briefwahlunterlagen sowie die Erfrischungsgelder werden den Ländern in Einzelabrechungen ersetzt, die übrigen Kosten sollen durch einen festen Betrag je Wahlberechtigten gedeckt werden. Bei Gemeinden bis 100.000 Wahlberechtigten beträgt dieser 0, 45 €, für Gemeinden mit mehr als 100.000 Wahlberechtigten 0, 70 € [§ 50 Absätze 2 und 3 BWG].

Für die Durchführung der Bundestagswahl 1998 betrug die Erstattung durch den Bund 58.439.000 € [vgl. Der Bundeswahlleiter 2005]. Allein für das benötigte Personal zur Vorbereitung, Durchführung und Nachbereitung der Wahl wurden durchschnittlich 66% der angefallenen Kosten aufgewandt [vgl. Stadt Braunschweig 2000, 4 ff.]. Neben einer Erstattung der Fahrtkosten haben die Wahlhelfer nach § 10 BWO einen Anspruch auf 16 € Erfrischungsgeld. Um genügend Wahlhelfer zu bekommen, sind viele Gemeinden jedoch gezwungen, höhere Beträge zu zahlen[146]. 12% der Gesamtkosten fielen auf Transport- und Portokosten, 10 % auf die Ausstattung und Bereithaltung der Wahlräume. Druckkosten und Büromaterial ebenso wie die allgemeine Datenverarbeitung benö-

[146] Im Land Bremen erhalten die Wahlhelfer beispielsweise 30 € Erfrischungsgeld. Vgl. http://www2.bremen.de/info/statistik/wahlen/wahlabc.htm (Verifizierungsdatum: 16.09.2005).

tigten jeweils 6% der Gesamtkosten [vgl. Stadt Braunschweig 2000, 4 ff.]. Der größte Anteil der Gelder wird somit durch den Personalaufwand bedingt. Bei den Bundestagswahlen 2002 fungierten 630.000 Wahlhelfer als Beisitzer der Wahlausschüsse und als Mitglieder der Wahlvorstände [vgl. Hanßmann 2003, 216].

Die internetbasierte Wahl bietet Möglichkeiten zur Kostensenkung in diversen Bereichen. Die Höhe der Reduzierung hängt jedoch maßgeblich davon ab, ob die herkömmlichen Wahlmöglichkeiten bestehen bleiben und in welchem Ausmaß öffentlich zugängliche Wahlcomputer bereitgestellt würden.

Die Größe der Wahlbezirke innerhalb eines Wahlkreises ist nach der BWO auf eine Größe von 2.500 Wahlberechtigten festgelegt, damit „allen Wahlberechtigten die Teilnahme an der Wahl möglichst erleichtert wird“ [§ 12 Absatz 2 BWO]. Bei einer Bundestagswahl kann mit rund 80.000 Wahllokalen gerechnet werden [vgl. Karpen 2005, 17]. Geht man davon aus, dass eine elektronische Wahl den gesamten Wahlablauf beschleunigt, indem z.B. die Identifizierung und der Abgleich mit dem Wählerverzeichnis automatisch durch die elektronische Signatur erfolgt, könnte die Anzahl der Wähler pro Wahlbezirk erhöht und damit die Anzahl der Wahllokale gesenkt werden. Durch diese Maßnahme konnte beispielsweise bei dem Einsatz elektronischer Wahlmaschinen in Dortmund zur Bundestagswahl 2002 die Anzahl der Wahllokale um 40% gekürzt werden. Die Anzahl der Wahlvorstände sank von ehemals 3.300 auf 2.000. Durch die damit verbundene Kostensenkung und einen multifunktionalen Einsatz der Wahlgeräte, z.B. bei Umfragen, rechnet sich der Anschaffungspreis nach ca. neun Wahlen [vgl. N.N. 2002b, 2]. Im Hinblick auf den Grundsatz der Allgemeinheit der Wahl begegnet die Reduzierung der Wahllokale jedoch Bedenken, da der Weg zum Wahllokal sich für einige Wahlberechtigte deutlich verlängert. Sind aber, wie z.B. in Köln in manchen Gebäuden mehrere Wahllokale untergebracht, um den Anforderungen des § 12 BWO zu genügen sowie die Stimmenauszählung pünktlich abzuschließen, ermöglicht der Einsatz elektronischer Wahlmaschinen die Reduzierung der Anzahl der Wahllokale, ohne ihre Erreichbarkeit einzuschränken [vgl. Kubicek & Wind 2002, 103].

Die internetbasierte Stimmabgabe (auch als optionale Alternative) lässt eine geringere Anzahl traditioneller Wahlmaterialien erwarten, da der Bedarf an herkömmlichen Stimmzetteln, deren Herstellung höhere Kosten verursacht als die der digitalen, sinkt. Bei der Übermittlung der elektronischen Voten entfielen ebenfalls das nach § 36 Absatz

4 BWG durch den Bund zu tragende Beförderungsgeld der Wahlbriefe sowie die Kosten für die Briefwahlumschläge.

Diesen möglichen Kosteneinsparungen stehen jedoch nicht unerhebliche Implementierungskosten gegenüber. Neben der Ausstattung der einzelnen Wahllokale mit Computern müssten die Wählerverzeichnisse digitalisiert sowie die technische Infrastruktur für die einzelnen Systemkomponenten finanziert werden. Hinzu kommen Schulungen für die Wahlhelfer sowie Support- und Serviceleistungen. Wenn pro Wahllokal lediglich jeweils ein Rechner für die Wähler und einer für die Wahlhelfer benötigt würden, entstünden hierfür Kosten in Höhe von ca. 160 Mio. €[147] [vgl. Karpen 2005, 17]. Demgegenüber stehen die Kosten der traditionellen Wahl von ca. 60 Mio. € [vgl. Der Bundeswahlleiter 2005]. Bislang ungeklärt ist die Frage, wer diese Kosten tragen sollte: der Bund, die Länder oder die Gemeinden. Nach § 50 BWG obliegt dem Bund die Übernahme der Kosten für Wahlen auf Bundesebene. Kämen die benötigten Geräte jedoch auf Gemeindeebene umfassend zum Einsatz, z.B. im Rahmen des E-Governments, wäre eine Anschaffung durch die Gemeinden in Betracht zu ziehen. Hierzu wäre allerdings eine umfassende Steigerung und Nutzung der E-Government-Angebote erforderlich.

Aus Wählersicht ist die herkömmliche Wahl mit einem sehr geringen Kostenaufwand verbunden. Eine internetbasierte Wahl dagegen, die auf der Identifizierung durch Chipkarten beruht, erfordert den Erwerb einer elektronischen Signatur sowie eines Kartenlesegeräts. Entscheidet sich der Wähler freiwillig für das E-Voting im individuellen Bereich als optionale Alternative, müsste er selber die Kosten für das nötige Equipment tragen [vgl. Karpen 2005, 33]. Sind Chipkarte und Lesegerät nur bei Wahlen verwendbar, scheint der Kosten-Nutzen-Faktor aus Wählersicht nicht gerechtfertigt. Bestünden jedoch auch andere Nutzungsmöglichkeiten, z.B. bei administrativen Behördengängen oder im Bereich des E-Commerce, wäre die Anschaffung attraktiver. Sollte einem Wähler aus anerkanntem Hinderungsgrund weder die Teilnahme an der Präsenz- noch an der Briefwahl möglich sein und E-Voting die einzige Option zur Ausübung seines Wahlrechts, müsste ihm der Zugang zu einem Computer sowie dem benötigten Equipment aufgrund des allgemeinen Wahlrechtsgrundsatzes ebenso wie die Briefwahl von staatlicher Seite finanziert werden. Interessant ist in dieser Hinsicht auch die estnische Varian-

[147] Hierbei wird von 1000 € pro Computer und 80.000 Wahllokalen ausgegangen; also 2*1000 € pro Wahllokal * 80.000 Wahllokale = 160 Mio. €.

te, bei der die elektronische Signatur generell in dem digitalen Personalausweis enthalten ist[148].

Ausgehend von der Annahme, dass neben der Internetwahl als optionale Alternative die Möglichkeit zur Präsenzwahl und zur Briefwahl bestehen bliebe, ist die Höhe der Einsparungen durch die elektronische Stimmabgabe wahrscheinlich begrenzt. So kommt auch der Schweizerische Bundesrat in erster Einschätzung zu dem Ergebnis, dass „die rein finanziellen Einsparungen [...] noch auf Jahrzehnte hinaus geringer bleiben [dürften] als die geschätzten Gesamtkosten“ [Schweizerischer Bundesrat 2002, 686]. Erst ein umfassendes Konzept, das E-Voting eng mit E-Government verknüpft, kann aufgrund der Anschaffungs- und Unterhaltungskosten zu merklichen Einsparungen führen.

4.2 Verlust der Wahlsymbolik

Die Einführung eines E-Voting-Systems kann neben technischen und rechtlichen Aspekten auch Einfluss auf das Ansehen von politischen Wahlen als grundlegenden Legitimationsmodus staatlicher Gewalt haben. Durch eine Technisierung des Wahlvorgangs könnten wichtige symbolische Funktionen, die den Wahlvorgang ritualisieren und auf denen das Vertrauen in ein sicheres Wahlsystem u.a. begründet ist, entfallen.

4.2.1 Öffentlichkeit

Die Öffentlichkeit der Wahl dient der Transparenz und Kontrolle des wichtigsten Legitimationsaktes der staatlichen Gewalt, gleichzeitig stellt sie einen wichtigen Ritus der Demokratie dar. Der Bürger kann sich durch den Gang zum Wahllokal öffentlich mit dem Staat identifizieren und seinen Willen zur Mitgestaltung der Staatsorgane manifestieren. Diese symbolische Funktion bleibt beim E-Voting im Wahllokal erhalten, in den Wahlkiosken tritt sie bereits zurück und bei der Fernwahl im individuellen Bereich entfiele sie ganz [vgl. Kerpen 2005, 55].

Während der Wahl spielt die Öffentlichkeit eine zentrale Rolle. So wie jeder Wahlberechtigte über das aktive und passive Wahlrecht verfügt, muss gleichzeitig jeder Bürger als Teil der Öffentlichkeit das Recht haben, den Wahlablauf als Zuschauer zu kontrollieren [vgl. Leder 2002, 653]. Diese Kontrolle wird also nicht nur durch den Wahlvorstand und die Wahlhelfer ausgeübt, sondern ist prinzipiell durch die BWO und das BWG jedem Bürger zugesichert. Während der Wahlvorbereitung werden Wahltermine

[148] Zur Umsetzung in Estland vgl. Kapitel 3.3.

und –orte öffentlich bekannt gegeben sowie Wählerverzeichnisse und Kandidatenlisten ausgelegt. Der Wahlakt ist in dem Sinne öffentlich, dass dessen freie Ausübung bei der Präsenzwahl ebenso wie die Auszählung der Stimmen und die Bekanntmachung der Wahlergebnisse beobachtet werden kann[149].

Beim E-Voting wird die Öffentlichkeit in den virtuellen Raum verlagert. Bei einer zusätzlichen Veröffentlichung der Wähler- und Kandidatenlisten und der Bekanntmachung der Wahltermine und –orte im Internet ist die Information leichter und schneller zugänglich. Im Fall einer internetbasierten Präsenzwahl im Wahllokal ist die Stimmabgabe der herkömmlichen Präsenzwahl gleichgestellt. Hier ergeben sich keine Veränderungen, da die freie Ausübung des Wahlaktes durch die Öffentlichkeit kontrolliert werden könnte, der eigentliche Wahlakt jedoch durch eine Wahlkabine geschützt ist. Die internetgestützte Fernwahl im individuellen Bereich wird von Kritikern als eine „Entführung der Politik aus dem öffentlichen Raum“ [Buchstein 2000a, 891] bezeichnet. Dies träfe jedoch nur zu, wenn E-Voting als Regelfall eingeführt würde. Gilt die Internetwahl jedoch als optionale Alternative neben der Präsenz- und Briefwahl, ist sie Letzterer gleichzusetzen. In beiden Fällen hat die Öffentlichkeit während des eigentlichen Wahlakts keine Kontrolle über die freie Ausübung des Wahlrechts.

Nach Beendigung der Wahl ermittelt der Wahlvorstand die Stimmen im Wahlbezirk öffentlich. Das Zustandekommen des Wahlergebnisses soll für den Bürger sowohl hinsichtlich der Präsenz- sowie der Briefwahl im Wahlbezirk wie auf Bundesebene nachvollziehbar sein [vgl. Karpen 2005, 32]. Dies gestaltet sich bei einer elektronischen oder internetgestützten Stimmenzählung problematisch. Selbst bei einer Offenlegung der Vorgänge innerhalb des Systems sowie des kompletten Programmiercodes ist die Funktionalität des komplexen Verfahrens für Laien nur schwer zu überprüfen. Die automatische Auszählung entzieht sich somit der Kontrolle durch die Öffentlichkeit, der Bürger muss auf die Aussagen der Experten vertrauen[150].

4.2.2 Geschwindigkeit

Die bei der Präsenzwahl im Wahllokal entstehende ‚Langsamkeit der Wahl’ sehen Kritiker im Fall des E-Votings aufgrund der mit der Computertechnologie verbundene Geschwindigkeit, mit der Entscheidungen artikuliert werden können, bedroht. Insbesonde-

[149] Vgl. § 10 BWG und § 31 BWG.
[150] Zu den Auswirkungen dieses eventuellen Vertrauensverlustes vgl. Kapitel 4.2.3.

re bei der Stimmabgabe im individuellen Bereich droht ein übereilter ‚Junk-Vote' [Buchstein 2000a, 891].

Durch den Gang ins Wahllokal entsteht eine zeitliche Spanne zwischen Information und Wahlakt, die eine kurzentschlossene, noch unter dem Eindruck der Wahlwerbung stehende Entscheidung ‚abkühlt'[151]. Durch die Digitalisierung und die Verlegung der Wahl in den individuellen Bereich verliert der Wahlakt jedoch „seinen symbolisch-rituellen Charakter und wird trivialisiert" [Kerpen 2005, 31]. Die Wahlentscheidung im individuellen Bereich kann prinzipiell schneller und unüberlegter getroffen werden; dies betrifft die Brief- ebenso wie die Internetwahl [vgl. Rüß 2002, 43f.]. Fernwähler können aufgrund kurzfristiger Informationen eine spontane, eventuell unreflektierte Wahlentscheidung treffen.

Interessant diesbezüglich scheint der Anteil der ungültig abgegebenen Erst- und Zweitstimmen bei den Briefwählern einerseits und den Präsenzwählern andererseits [vgl. Schwartzenberg & Geiert 2002, 646]. Bei den Bundestagswahlen 2002 wurden 1, 0% der Erst- und 0, 6% der Zweitstimmen der Briefwähler ungültig gewertet. Dagegen waren 1, 6% bzw. 1, 3% der Präsenzwahlstimmen ungültig [vgl. Der Bundeswahlleiter 2005]. Begründet wird der niedrige Anteil ungültiger Stimmen der Briefwähler mit der Umgebung der Stimmabgabe im individuellen Bereich. Gerade bei der Stimmabgabe außerhalb des Wahllokals kann der Wähler sich mehr Zeit und Ruhe zum Lesen der Hinweise und Ausfüllen des Stimmzettels nehmen [vgl. Schwartzenberg & Geiert 2002, 647]. Dies ließe sich auf die Internetwahl im individuellen Bereich übertragen. Zusätzlich könnte man davon ausgehen, dass der Wähler sich im individuellen Bereich nicht nur mehr Zeit zum korrekten Ausfüllen des Stimmzettels nimmt, sondern auch für die Wahlentscheidung als solche. Allein die bei der Fernwahl bestehende Möglichkeit zur freiwilligen Aussetzung von Wahlpropaganda lässt nicht auf eine generell unüberlegte und übereilte Stimmabgabe schließen.

Die Wahl im Internet verstärkt dennoch die Gefahr der unüberlegten Stimmabgabe, da diese ohne Medienbruch zeitlich direkt im Anschluss an die Informationsphase erfolgen kann. Das in § 32 BWG normierte Verbot von Wahlpropaganda sollte daher auch bei der internetbasierten Präsenzwahl angewendet und dahingehend ausgeweitet werden, dass ausschließlich die offizielle Wahlseite aufgerufen werden kann. Im individuellen

[151] Vgl. § 32 BWG zum Verbot der Wahlwerbung in, an und vor dem Wahllokal.

Bereich müsste der Wähler die medienbedingte Geschwindigkeit selbst kontrollieren und wäre für eine freie, reflektierte Stimmabgabe eigenständig verantwortlich [vgl. Karpen 2005, 56]. Bezüglich der oben erwähnten Aspekte gemäß der Ungültigkeitsquote der Briefwahl, ist damit zu rechnen, dass sich Wähler im individuellen Bereich, unabhängig vom Medium, Zeit für den Wahlakt nehmen. Zusätzlich lässt sich die Stimmabgabe durch Maßnahmen innerhalb des Programms verlangsamen. Eine Plausibilitätskontrolle den Inhalt der Stimme betreffend, so dass das Votum erst nach einer erfolgten Bestätigung abgeschickt werden kann, verzögert den Wahlvorgang automatisch. Die Gefahr einer übereilten und unreflektierten Stimmabgabe ist somit bei einem E-Voting-System grundsätzlich nicht größer als bei der herkömmlichen Wahl.

4.2.3 Vertrauen in E-Voting als ‚sicheres Wahlverfahren'

Das traditionelle Wahlverfahren hat sich seit seiner Einführung als ‚sicheres Verfahren' bewährt und genießt aufgrund dessen bei Wahlveranstaltern und der Wahlbevölkerung breite Akzeptanz und Vertrauen [vgl. Birkenmaier m.w.N. 2004, 78]. Dieses Vertrauen kann jedoch nicht ausschließlich mit den getroffenen Sicherheitsvorkehrungen begründet werden. Die Sicherung der einzelnen Wahllokale sowie die Identifizierung der einzelnen Wähler[152] sind unzureichend; Manipulationsmöglichkeiten ergeben sich u.a. auch bei der Beförderung der gut zu erkennenden Wahlbriefe. Prinzipiell baut das traditionelle Wahlsystem folglich auf einem naiven Sicherheitskonzept auf. Es wird im Allgemeinen dennoch aufgrund der Loyalität der Wahlberechtigten als Staatsbürger, des Vertrauens in die ethische und politische Integrität der verantwortlichen Wahlvorstände und –helfer, der Kontrolle durch die nach politischem Proporz zusammengesetzten Gremien und der Angst vor den Sanktionen des Strafrechts bezüglich Wahlvergehen als sicher wahrgenommen [vgl. Otten 2002, 72].

Fraglich ist, inwieweit sich die Akzeptanz der Bürger bei Einführung eines neuen Wahlsystems verändern würde. Das Vertrauen der Wahlberechtigten in die Rechtmäßigkeit einer Wahl ist unabdingbar für die Legitimation einer Regierung. In der Umfrage zur ‚Akzeptanz virtueller Behörden-Dienstleistungen und Einstellungen zu Wahlen über das Internet' der ‚inra Deutschland'[153] im Jahr 2000 bewerteten knapp die Hälfte der Be-

[152] Nach § 56 Absatz 3 BWO hat sich der Wähler nur auf Verlangen des Wahlvorstandes auszuweisen.
[153] Die Studie ist online nicht mehr verfügbar und wird im Folgenden nach [Hanßmann 2003, 225ff] zitiert.

fragten (48%) die Möglichkeit zur Teilnahme an politischen Wahlen im Internet positiv, somit scheint ein grundlegendes Vertrauen vorhanden zu sein.

	Total	Geschlecht		Altersgruppen					Schulbildung		
		Frauen	Männer	14-24	25-34	35-44	45-64	65+	Volksschule	Real-/Fachschule	Abitur/Uni
	1000	523	477	141	160	173	324	202	312	355	328
Würde ich sehr begrüßen (+3)	25%	26%	25%	18%	35%	25%	26%	23%	27%	25%	24%
(+2)	15%	15%	15%	22%	14%	15%	14%	13%	14%	16%	15%
(+1)	8%	8%	8%	11%	8%	10%	7%	8%	7%	9%	9%
(0)	11%	12%	11%	22%	8%	14%	10%	7%	6%	10%	18%
(-1)	4%	5%	2%	1%	5%	5%	4%	3%	6%	3%	3%
(-2)	10%	11%	10%	8%	9%	11%	8%	15%	9%	11%	10%
(-3)	23%	20%	27%	18%	19%	20%	28%	24%	24%	23%	22%
o.A.	3%	3%	3%	1%	2%	1%	3%	7%	6%	3%	0%

Abbildung 7: Zustimmung zur Internet-Stimmabgabe bei Wahlen [Hanßmann 2003, 226].

Die meisten Befürworter der Einführung von Internetwahlen sind in der Gruppe der 25-34jährigen zu finden. Mit zunehmendem Alter sinkt die Akzeptanz. Wenig Einfluss auf die Einstellung gegenüber dem E-Voting hat hingegen der Grad der formellen Bildung. Ein ähnliches Ergebnis lässt sich bei der Umfrage der Wirtschaftswoche und des Meinungsforschungsinstituts TNS Emnid ablesen: 50% der Befragten würden ihre Stimme im Internet abgeben. 43% der Nichtwähler unter den Befragten stimmten der Aussage zu, dass sie regelmäßiger wählen würden, wenn dies online möglich wäre [vgl. Losse 2000]. Die Hintergründe der Einschätzungen der Befragten wurden in beiden Umfragen nicht berücksichtigt.

Maßgebend für die Akzeptanz eines E-Voting-Systems ist das Vertrauen der Wähler in die rechtmäßige Funktionalität des Systems. Prinzipiell sollte das Vertrauen in ein technisches System auf dem diesem System zugrundeliegenden theoretischen, wissenschaftlich abgesicherten und dementsprechend realisierten Wissen beruhen. Ist der Zugang zu diesem Wissen jedoch verwährt, muss die Vertrauenssicherung durch andere Komponenten geleistet werden [vgl. Kuhlen 1999, 93]. Um diese herauszufinden, wurden bei einer transnationalen Untersuchung fünfzehn Feldstudien in vier verschiedenen Ländern[154] zu dem Umgang und Vertrauen der Probanden gegenüber einem E-Voting-System durchgeführt [vgl. Oostveen & van den Besselaar 2004, 73ff.]. Das Testsystem stellte für den Wähler keine Möglichkeit bereit, die erfolgreiche Übermittlung der

[154] Die Feldstudien wurden in Newham (England), Orsay (Frankreich), einer CGIL-Gewerkschaftsniederlassung in Mailand (Italien) und in zwei Community-Networks in Italien und Finnland durchgeführt.

Stimme zu kontrollieren. Auf dem Bildschirm wurde lediglich vor Abschicken der Stimme eine Plausibilitätskontrolle durchgeführt. Dennoch gaben 61% der Testwähler an, es sei für sie ‚very easy' gewesen, die korrekte Speicherung der Stimme zu überprüfen. Nur 5, 8% stimmten dieser Aussage nicht zu. Zur Evaluierung der Hintergründe dieses Vertrauens wurden die Aussagen in Korrelation zu persönlichen Daten und Eigenschaften der Testwähler sowie den Rahmenbedingungen der Testwahl gesetzt. Der Grad der Dezentralisierung hatte keinen Einfluss auf die Aussage. Das Alter und die Geschlechtszugehörigkeit waren ebenfalls nicht ausschlaggebend für das entgegengebrachte Vertrauen. Überraschend ist, dass auch die Medienkompetenz keinen relevanten Unterschied erkennen ließ. So wäre zu vermuten, dass regelmäßige Computernutzer mehr über die Risiken in Netzwerken wüssten. Die Wähler, die neuen Informations- und Kommunikationstechniken gegenüber generell aufgeschlossen sind, bringen diesen auch mehr Vertrauen entgegen.

Allgemein vertrauten die Testwähler eher der sicheren Übermittlung und Speicherung ihres Votums als der Sicherheit der Verwendung der persönlichen Daten. Bereits bei der zur Beantragung der digitalen Signatur erforderlichen Angaben persönlicher Daten gab die Mehrheit der Testwähler an, sie habe Sorge, dass diese weitergeleitet und später nicht von ihrer Stimme entkoppelt würden. Interessant ist auch, dass diejenigen, die die Wahl als Bürgerpflicht anerkennen, die Einführung eines E-Voting-Systems eher befürworten als Nichtwähler. Dies kann aber mit der Bedeutung in Zusammenhang stehen, die der Einzelne der Wahl an sich als erforderlicher Komponente eines demokratischen Systems entgegenbringt.

Die Studie zeigt, dass die Testwähler dem System bezüglich der korrekten Stimmenübermittlung und –speicherung vertrauten, ohne sich tatsächlich von den technischen Umsetzungen überzeugen zu können. Der Aufbau von Vertrauen scheint somit auf anderen, nicht technik-basierten Komponenten begründet zu sein. Die Befragungen und Untersuchungen, die zu den Pilotprojekten[155] der Forschungsgruppe Internetwahlen durchgeführt wurden, verdeutlichen, dass das Vertrauen in die Sicherheit der Technik hauptsächlich über Vertrauen in Institutionen und Personen aufgebaut wird [vgl. Ellermann 2004, 34]. Waren die Wahlvorstände von dem System überzeugt und verwiesen zusätzlich auf die erfolgreiche Prüfung des Systems durch den jeweiligen Datenschutz-

[155] Zu den Pilotprojekten der Forschungsgruppe Internetwahlen vgl. Kapitel 3.4.1.

beauftragten, reichte dies als vertrauensbildende Maßnahme aus. Vertrauen wird somit auch durch die Delegation an Experten aufgebaut, denen das nötige Wissen über und das Beherrschen der Systeme zugesprochen wird. Dabei müssen die Experten ihr Wissen nicht öffentlich präsentieren, ihre Position innerhalb des Systems oder einer Institution scheint auszureichen [vgl. Kuhlen 1999, 101f.]. Dennoch kann die Offenlegung des Quellcodes als eine vertrauenfördernde Maßnahme wirken, da so vermittelt wird, das bei entsprechendem Fachwissen die Abläufe im System nachvollziehbar wären [vgl. Rüß 2002, 46]. Zusätzlich käme die Förderung vertrauensbildender Transformationsleistungen durch öffentliche Qualitäts- und Sicherheitskontrollen durch neutrale Instanzen und Institutionen in Betracht [vgl. Kuhlen 1999, 102]. Die verwendeten Systeme sollten durch eine offizielle Zertifizierungs- und Prüfstelle ausgezeichnet werden[156]. Auch wenn die Prüfung der Öffentlichkeit aufgrund fehlenden Expertenwissens bei den Wählern somit nicht während der Wahl erfolgen kann, wird diese Aufgabe durch eine Institution im Vorfeld der Wahl übernommen.

Wichtig für den Aufbau von Vertrauen gegenüber der neuen Wahlmöglichkeit sind auch der erwartete persönliche Nutzen des Wählers und die generelle technische Innovationsbereitschaft [vgl. Ellermann 2004, 33]. Die verschiedenen Wahlmöglichkeiten sind aus Wählersicht unterschiedlich effizient. Hierbei spielt der Grad der Dezentralisierung sowie die erforderlichen Mittel und Kompetenzen eine große Rolle. Müsste der Wähler sich zunächst die nötige Medienkompetenz sowie die erforderliche technische Ausstattung aneignen und bräuchte diese nur für die Wahl, könnte die Entscheidung allein aus praktischen Gründen gegen die neue Wahlmöglichkeit ausfallen. Könnte er jedoch nicht an der Präsenzwahl teilnehmen und böte die Internetwahl gegenüber der Briefwahl Vorteile, wie z.B. das Entfallen der Voraus-Wahl, käme dem E-Voting eine größere Effizienz zu. Dies könnte sich wiederum auf das Vertrauen auswirken, da eine Steigerung des persönlichen Nutzens zugleich eine Steigerung der Bereitschaft, einer neuen Technik zu vertrauen, mit sich bringt [vgl. Oostveen & van den Besselaar 2004, 81]. Beeinflusst wird der Vertrauensaufbau zusätzlich von der persönlichen Innovationsbereitschaft. Die Neugier gegenüber neuen Verfahren basiert einerseits auf einer positiven Einstellung zu Technik, andererseits auf dem Vertrauen in die eigenen Kompetenzen im Umgang mit einer neuen Technik [vgl. Ellermann 2004, 37].

[156] So können auch nur Wahlgeräte eingesetzt werden, die durch die Physikalisch-Technische Bundesanstalt geprüft und durch das Bundesinnenministerium zugelassen sind. Vgl. § 1 WahlGVO.

Das Vertrauen in ein Wahlsystem hängt nicht zuletzt ab von der Möglichkeit, das Wahlergebnis im Nachhinein zu kontrollieren. Die nachträgliche Wahlprüfung gemäß Artikel 41 GG erfordert eine Stimmenspeicherung, die eine mehrfache Auszählung ermöglicht. Dies ist technisch ohne Probleme durchführbar, beinhaltet jedoch keine Kontrollmöglichkeit für den Wähler. Durch einen ‚Audit-Trail' [Oostveen & van den Besselaar 2004, 74] in Form einer Quittung, die der Wähler nach seiner Stimmabgabe direkt an seinem Wahlcomputer ausdruckt, überprüft und in eine Urne wirft[157], könnte ein Abgleich mit den elektronischen Stimmen erfolgen. Dies böte in zweifacher Hinsicht Vorteile: einerseits ist die Prüfung der elektronischen Stimmen im Nachhinein im Falle technischen Versagens zusätzlich manuell möglich, andererseits kann der Wähler durch den Abgleich darauf vertrauen, dass seine Stimme gezählt wurde.

Zu einer weitreichenden Akzeptanz des neuen Wahlmodus' ist es erforderlich, vertrauensbildende Maßnahmen zu ergreifen, die die obengenannten Aspekte berücksichtigen. Anzustreben ist der Austausch von Informationen zwischen Experten und Wahlberechtigten mithilfe der Massenmedien. Durch die Kommunikation kann ein ‚Vertrauensnetzwerk' [Kuhlen 1999, 103] entstehen, das die Systemverantwortlichen sowie die von dem System ‚Betroffenen' (die Wahlberechtigten) einschließt. Durch gezielte Förderung der Medienkompetenz der Wähler in Vorbereitungskursen kann zusätzlich das Vertrauen in die eigenen Fähigkeiten im Umgang mit Wahlcomputern gesteigert werden[158].

4.3 E-Voting als Mittel zur Steigerung der Wahlbeteiligung

Gemäß Artikel 20 Absatz 2 GG legitimiert das Volk durch rechtmäßige Wahlen seine Regierung. Angesichts der allgemein diagnostizierten ‚Politikverdrossenheit' und sinkender Wahlbeteiligung stellt sich die Frage nach der formalen Legitimation der Regierung. Mit steigender Zahl der Nichtwähler entsteht ein Parlament, das nur von einem Teil der Bevölkerung gewählt wurde, aber für alle Bürger Entscheidungen trifft.

Bei den Bundestagswahlen ist, mit Ausnahme von 1998, seit den siebziger Jahren ein stetiger Rückgang der Wahlbeteiligung zu verzeichnen. Im Jahr 2002 gaben 79, 1% der Wahlberechtigten ihre Stimme ab, d.h. gut ein Fünftel der Wahlberechtigten nahm sein

[157] Der Wähler darf die Quittung unter keinen Umständen behalten, da sie einen Beweis der Wahlentscheidung darstellt und somit die freie Wahl gefährden würde.
[158] Vorschläge zur Förderung der Medienkompetenz vgl. Kapitel 5.1.3.

Stimmrecht nicht in Anspruch [vgl. Der Bundeswahlleiter 2003, 1]. Bei Landtags- und Kommunalwahlen ist der Rückgang noch gravierender. Sachsen-Anhalt stellte 2004 einen neuen Negativrekord auf; die Beteiligung an den Kommunalwahlen lag durchschnittlich bei 42, 2%[159]. Vor dem Hintergrund der stetig wachsenden Anzahl der Internetnutzer, unter denen die ‚politikverdrossenen' Jugendlichen und jungen Erwachsenen besonders stark vertreten sind [vgl. Eimeren et al. 2004, 340], wird die Einführung internetbasierter Wahlen als Lösung dieses Legitimationsproblems diskutiert [vgl. Hanßmann m.w.N. 2003, 199].

Der Grund für die sinkende Wahlbeteiligung ist nur schwer auszumachen. Durch die Möglichkeit der Briefwahl ist eine flexible Alternative zur Präsenzwahl geschaffen worden; die Aufteilung der Wahlbezirke wirkt sich positiv auf relativ kurze Wege zum Wahllokal und auf geringe Wartezeiten aus. Nach § 16 BWG ist der Wahltag zudem auf einen Sonntag oder einen gesetzlichen Feiertag zu legen, der für die Mehrheit der Bevölkerung kein Arbeitstag ist. Der zeitliche Aspekt kann somit kaum die Hauptursache für die mangelnde Wahlbeteiligung darstellen [vgl. Hanßmann 2003, 203]. Vielmehr scheint es eine Gruppe Nichtwähler zu geben, für die sich der Aufwand des Wahlaktes persönlich nicht lohnt. In einer Studie der Bertelsmann Stiftung zur ‚Politischen Partizipation in Deutschland' gaben über die Hälfte der Befragten an (51%), dass es für sie keinen großen oder überhaupt keinen Unterschied mache, wer im Bund regiert; 60% darunter zählten sich selber zu selten oder nie wählenden Bundesbürgern. Zusätzlich wirkt sich die Relevanz, die den verschiedenen Parlamentsebenen zugesprochen wird, auf das Wahlverhalten aus. Die Entscheidungen des Bundestages werden mehrheitlich als relevant eingestuft (85%), die Vorgänge in Land- und Stadt- oder Gemeinderat beurteilte knapp ein Drittel der Befragten als weniger wichtig bzw. unwichtig. Insofern ist die Nichtwahl zumindest teilweise Ausdruck politischer Verdrossenheit; sie bezieht sich jedoch mehr auf politische Akteure und aktuelle Geschehnisse als auf die Staatsform der Demokratie, die vom Großteil der Befragten (77%) nicht in Frage gestellt wird [vgl. Bertelsmann Stiftung & Forschungsgruppe Wahlen 2004, 54f.].

[159] Vgl. Sozialdemokratische Gemeinschaft für Kommunalpolitik (SGK) unter http://www.sgk-online.net/servlet/PB/menu/1109464/ (Verifizierungsdatum: 16.09.2005).

Die Motivstruktur der Nichtwähler ist heterogen, sie wird u.a. durch den sozioökonomischen Status[160], das Alter, die soziopolitische Integration (z.B. Vereinsmitgliedschaft, Gewerkschaftsmitgliedschaft), das Niveau der formalen Bildung, die politische Orientierung (z.B. politisches Interesse, Parteienidentifikation) und Kommunikation (z.B. Mediennutzung) beeinflusst [vgl. Niedermayer 2001, 164ff.]. Ein gruppen- und milieuübergreifender Faktor ist dagegen die Anerkennung der Wahl als staatsbürgerliche Pflicht, deretwegen auch politisch weniger Interessierte öfter an der Wahl teilnehmen. Durch die wachsende Normalisierung und Festigung des demokratischen Systems nach 1949 verliert die Wahlnorm jedoch zunehmend an Bedeutung [vgl. Niedermayer 2001, 175].

Die durchgeführten Pilotprojekte lassen keine auf die Einführung des E-Votings zurückzuführende signifikante Steigerung der allgemeinen Wahlbeteiligung erkennen. Jedoch zeigt sich, dass die internetgestützte Wahl im individuellen Bereich weitgehend sehr positiv angenommen, die Wahl in Wahlkiosken hingegen schlecht frequentiert wird[161]. Der Großteil der E-Voter lässt sich jedoch nicht der Gruppe der bisherigen Nichtwähler zuordnen.

Neben der formalen Legitimation ist auch die inhaltliche Legitimation der Regierenden von Bedeutung [vgl. Schreiber 2002, 31]. Fraglich ist daher, ob bei der ‚politischen Apathie' der Nichtwähler eine vermeintlich bequemere Stimmabgabe über das Internet tatsächlich eine Lösung für das Problem der sinkenden Wahlbeteiligung bietet. Die Identifikation mit politischen Handlungsträgern setzt einen politischen Willensbildungsprozess der Wähler voraus; dies lässt sich bei den beschriebenen Aussagen der Nichtwähler nicht erkennen. Selbst wenn der Zugang zur Wahl beispielsweise durch eine internetbasierte Fernwahl im individuellen Bereich, gegebenenfalls sogar ohne Antragsstellung, die formale Legitimation steigern könnte, ist fraglich, ob dies gleichzeitig einer inhaltlichen Legitimation entsprechen würde.

Die stetig wachsende Verbreitung und Popularität des Internets lässt dennoch vermuten, dass eine Internetwahl große Aufmerksamkeit auf sich ziehen würde. Insbesondere jun-

[160] Während knapp die Hälfte der regelmäßigen Wähler ihre eigene finanzielle Lage als gut einstuft, halten über ein Drittel der Nichtwähler ihre persönliche Wirtschaftslage für schlecht. Vgl. [Bertelsmann Stiftung 2004, 129].

[161] Vgl. Kapitel 3.2 zu den Pilotprojekten in Großbritannien, bei denen fünfmal so viele Internetwähler an der internetbasierten Fernwahl im individuellen Bereich teilnahmen als an den bereitgestellten Wahlkiosken.

ge Nichtwähler könnten dies zum Anlass nehmen, sich an der Wahl zu beteiligen. Neugier und Interesse bieten jedoch keine langfristige Lösung für eine Steigerung der Wahlbeteiligung, da der ‚Reiz des Neuen' nicht dauerhaft wirkt.

Das Potential des E-Votings, die Wahlbeteiligung zu steigern, scheint daher begrenzt. Zwar kann die Möglichkeit der internetbasierten Stimmabgabe die Wahlbeteiligung erhöhen, wenn eine Wahl auch außerhalb des heimischen Wahllokales möglich ist, essentiell ist aber auch, die Motivation der Nichtwähler zu steigern. Bürger, die sich in lokalen Vereinen, Bürgerinitiativen oder Interessensgemeinschaften engagieren, interessieren sich tendenziell mehr für Politik, beteiligen sich häufiger an Wahlen und zeigen eine grundsätzlich positivere Haltung gegenüber der Demokratie als Nicht-Aktive [vgl. Bertelsmann Stiftung & Forschungsgruppe Wahlen 2004, 131]. Freiwilliges und politisches Engagement scheinen durch eine sich gegenseitig verstärkende Wechselwirkung verbunden zu sein. Maßnahmen zur Förderung von Bürgerbeteiligung können also tendenziell zwei Zielen dienen: der Stärkung des bürgerschaftlichen Engagements und der Stärkung des politischen Interesses. Das Medium Internet ist in den Bereichen der Partizipation durch die Bürger besonders geeignet[162]. Besonders in den Phasen direkt vor einer Wahl sollte das Internet durch die Kandidaten verstärkt für die Kommunikation mit den Bürgern genutzt werden, schwerpunktmäßig in Chats und Foren. Die Relevanz der Themen könnte durch das Gefühl ‚gefragt zu werden' steigen. In Estland werden Parlamentssitzungen live im Internet übertragen[163], auch in Deutschland gibt es erste Online-Parteitage[164], bei denen auch Nicht-Mitglieder mitdiskutieren und Anträge stellen können [vgl. Karpen 2005, 13]. Inszenierte Fernsehereignisse wie das ‚Kanzlerkandidatenduell' verfolgten zur Bundestagswahl 2002 15 Mio. Zuschauer [vgl. Hebecker 2002, 1], zur Bundestagswahl 2005 sogar 21 Mio. [vgl. Segler 2005]. Zu derartigen Ereignissen könnten im Internet Diskussionsforen in Echtzeit angeboten werden, um auch den Kommunikationsprozess der Bürger untereinander zu fördern.

Der Ausbau der interaktiven Information, Kommunikation und Partizipation des politischen Prozesses im Internet ist auch unabhängig von der Einführung des E-Votings ein vielversprechendes Konzept, das sich positiv auf die Wahlbeteiligung auswirken könnte, wenngleich anzunehmen ist, dass die Möglichkeit der Stimmabgabe ohne Medien-

[162] Zu den Funktionen des Internets für die Demokratie vgl. Kapitel 1.2.2.
[163] Zu Estland vgl. Kapitel 3.3.
[164] Vgl. z.B. http://www.virtueller-parteitag.de/medien/online.html (Verifizierungsdatum: 16.09.2005).

bruch die Attraktivität dieser Angebote zusätzlich steigert. Die alleinige Einführung einer weiteren Beteiligungsmöglichkeit an der Wahl würde der ‚Politikverdrossenheit' und der sinkenden Wahlbeteiligung somit wahrscheinlich nicht entgegen zu wirken vermögen.

5 E-Voting in Deutschland?

5.1 Umgang mit dem Problem der digitalen Spaltung

Der Begriff der digitalen Spaltung beinhaltet zwei Dimensionen: eine weltpolitische und eine national-gesellschaftspolitische [vgl. Marr 2005, 25]. Erstere bezieht sich auf das Gefälle der Nutzungsmöglichkeiten bezüglich der Informations- und Kommunikationstechnologien zwischen Industrienationen, Schwellenländern und Entwicklungsländern. Letztere beschäftigt sich im Gegensatz dazu mit den Auswirkungen der Verbreitung und Nutzung des Internets im Hinblick auf die Teilung einer nationalen Gesellschaft in ‚Informationseliten' und ‚Habenichtse' [Leggewie 1998, 40]. Im Folgenden werden die national-gesellschaftspolitische Dimension in Deutschland und ihre etwaigen Konsequenzen im Fall der Einführung des E-Votings analysiert.

Schwerpunkt der Diskussion um eine digitale Spaltung war bislang der technische Zugang zum Internet. Diese Betrachtung lässt die Nutzerperspektive, wie beispielsweise Benutzerfreundlichkeit, Kosten, Handhabbarkeit sowie Kompetenz im Umgang mit dem Medium, außeracht [vgl. Gehrke & Tekster 2004a, 1]. Die digitale Spaltung umfasst nicht nur die Verbreitung der technischen Zugänge, sondern auch eine gesellschaftliche Zweiteilung in On- und Offliner, also in jene, die nutzen und jene, die nicht nutzen (können). Probleme hinsichtlich der hier diskutierten Fragestellung entstehen jedoch erst, wenn der Zugang und die Nutzung des Internets umfassendere Möglichkeiten zur politischen Information und Teilnahme bieten.

5.1.1 Verbreitung und Nutzung des Internets

Im Jahr 2004 gebrauchten 55, 3 % der deutschen Bevölkerung ab 14 Jahren zumindest gelegentlich das Internet[165]; hochgerechnet entspricht dies 35, 7 Mio. [vgl. Eimeren et al. 2004, 351]. Unter den Wahlberechtigten zählen sich nur 51 % zu den regelmäßigen Internetnutzern [vgl. Initiative D^{21} 2004, 15]. Somit ist fast die Hälfte dieses Bevölkerungsteils von dem Medium ausgeschlossen. Zwischen der Gruppe der Nutzer und der Gruppe der Nichtnutzer lassen sich soziodemographische Tendenzen ausmachen.

[165] Aufgrund verschiedener methodischer Vorgehensweisen differieren die Ergebnisse unterschiedlicher Studien leicht, in der Tendenz sind sie jedoch vergleichbar. Die folgenden Aussagen stützen sich auf die ARD/ZDF-Online-Studie 2004 [Eimeren et al. 2004] sowie den (N)Onliner Atlas 2004 [Initiative D^{21} 2004].

In der Gruppe der über 39jährigen sind durchschnittlich 80 % online, doch auch die Hälfte der bis 60jährigen gehört zu den Internetnutzern. Nur in den höheren Altersgruppen zählen die Onliner noch zur Ausnahme: lediglich ein Viertel der über 60jährigen und knapp ein Zehntel der über 70jährigen nutzt das Internet. Von Bedeutung ist auch die Geschlechtszugehörigkeit. 60 % der Männer und 45 % der Frauen rechnen sich zu den regelmäßigen Onlinern. Neben Alter und Geschlechtszugehörigkeit spielen vor allem Bildung und Prosperität eine Rolle. Schüler, Abiturienten und Hochschulabsolventen scheinen das Medium fast flächendeckend in ihren Alltag integriert zu haben; durchschnittlich knapp 80 % von ihnen zählen zu den regelmäßigen Nutzern. Im Gegensatz dazu stehen nur ein Fünftel der Hauptschulabsolventen. Dass sich die Internetnutzung im privaten Bereich auch am Haushaltsnettoeinkommen orientiert, ist aufgrund der Anschaffungs- und Zugangskosten zu vermuten. In der Gruppe der Besserverdienenden (>2.500 €) sind gut 70 % online, während sich in den niedrigen Gehaltsgruppen (<1000 €) nur ein Viertel zu den Internetnutzern zählen lässt. Die Internetnutzung am Arbeitsplatz ist fast flächendeckend festzustellen, allein unter den einfachen Arbeitern und Handwerkern ist noch jeder zweite am Arbeitsplatz Nichtnutzer. Bei den Nichtberufstätigen hat sich das Internet noch nicht etabliert. Nur 37 % der Hausfrauen/männer und 16 % der Rentner nutzen das Internet regelmäßig [vgl. Initiative D^{21} 2004, 12ff.].

5.1.2 Mögliche Auswirkungen der digitalen Spaltung auf das E-Voting

Im Hinblick auf Beteiligungsmöglichkeiten im Internet verwehrt die digitale Spaltung den Offlinern den Zugang zu einem Teil der bestehenden Möglichkeiten, am politischen Willensbildungsprozess teilzunehmen und, bei einer flächendeckenden Einführung des E-Votings, ihren Willen zu äußern.

Soweit die Nichtnutzung des Internets allein auf mangelnden technischen Zugangsmöglichkeiten begründet ist, ist zunächst festzuhalten, dass Artikel 87f GG, der den Bund verpflichtet, im Bereich von Postwesen und Telekommunikation flächendeckend angemessene und ausreichende Dienstleistungen zu gewährleisten, nicht die Pflicht zur Gewährleistung von Internetzugängen beinhaltet [vgl. Birkenmaier 2004, 290]. Der technische Zugang zum Internet am Wahltag könnte dennoch weitgehend durch öffentlich zugängliche Terminals gesichert werden. Von einer etwaigen Versorgungslücke betroffene Wähler könnten auf die klassischen Wahlmöglichkeiten verwiesen werden, da die-

se bereits den Allgemeinheitsgrundsatz wahren[166]. Entscheidet sich der Wähler für E-Voting in Form der Fernwahl, gewährt Artikel 87f GG gleichfalls keinen Anspruch auf die Bereitstellung eines technischen Zugangs zum Internet. Für die Verfügbarkeit des erforderlichen Equipments hat der Wähler eigenständig zu sorgen[167].

Unabhängig von der Frage der technischen Verbreitung des Internetzugangs wäre ein Teil der Nichtnutzer allein aufgrund mangelnder Medienkompetenz von der internetgestützten Wahl ausgeschlossen. Mangelnde Medienkompetenz scheint nicht unter die Hilfsbedürftigkeit des § 33 Absatz 2 BWG zu fallen, so dass die Offliner keinen Anspruch auf eine Hilfsperson zur gültigen Stimmabgabe hätten. Die aus der Inkompetenz resultierende Ungleichheit der Teilnahmemöglichkeiten an der Wahl steht dennoch in Einklang mit den Wahlrechtsgrundsätzen, da Offliner die Möglichkeit zur ohnehin maßstabsbildenden Präsenzwahl[168] sowie gegebenenfalls zur Fernwahl in Form der Briefwahl haben.

Internetwähler sind gegenüber Präsenz- und Briefwahlnutzern dennoch im Vorteil. Zum einen verdeutlicht ein Vergleich von Brief- und Internetwahl, dass der zeitliche Entscheidungsrahmen bei Letzterer dem der Präsenzwahl entspricht. Bei der Briefwahl hingegen ist eine Voraus-Wahl zu treffen, so dass die den Briefwählern zur Verfügung stehende Zeitspanne, ihre Entscheidung zu fällen, kürzer ist. Zudem steht Onlinern im Rahmen des politischen Willensbildungsprozesses mit dem Internet ein zusätzlicher Informationskanal[169] zur Verfügung. Auch wenn fraglich und empirisch schwer zu belegen ist, inwieweit Onliner das Internet tatsächlich zur qualitativen politischen Informationsgewinnung einsetzen [vgl. Marr 2005, 77], verfügen sie jedenfalls aus Übungsgründen über die erforderliche Medienkompetenz. Zwar ist zu bedenken, dass weder ein Rechtsanspruch auf Nutzung des Internets zur Informationsgewinnung, noch auf Teilnahme an der Internetwahl als Fernwahl besteht, dennoch sind die ungleichen Nutzungsmöglichkeiten des Internets für demokratische Prozesse einzudämmen, indem die erforderliche Medienkompetenz einer- sowie die technischen Zugänge andererseits gezielt gefördert werden.

[166] Zur allgemeinen Wahl vgl. Kapitel 2.3.1.
[167] Zur allgemeinen Wahl vgl. Kapitel 2.3.1.
[168] Zur allgemeinen Wahl vgl. Kapitel 2.3.1.
[169] Zur Informationsfunktion des Internets im politischen Willensbildungsprozess vgl. Kapitel 1.2.2.1.

5.1.3 Vorschläge zur Minderung der digitalen Spaltung

Die Minderung der digitalen Spaltung setzt primär die Schaffung einer breiteren Akzeptanz des Mediums Internet voraus. Beachtung ist insbesondere den Bevölkerungsgruppen zu schenken, die bisher mehrheitlich offline sind. Dies erfordert die Schaffung von Rahmenbedingungen, die sowohl ‚harte' als auch ‚weiche' Infrastrukturfaktoren beinhalten [vgl. Initiative D^{21} 2000, 9]. Unter die ‚harten' Faktoren fällt z.B. die technische Ausstattung, während die ‚weichen' Faktoren die Förderung der Medienkompetenz in Form von Aus- und Weiterbildung, die Schaffung eines rechtlichen Rahmens und „die Vorbildfunktion des Staates bei der Nutzung von Online-Diensten" [ebd.] beinhalten. Durch ein Konzept der Zusammenarbeit von öffentlichen Stellen, privaten Unternehmen und Non-Profit-Organisationen könnten technische Zugänge in Form von Computern mit Internetzugang bereitgestellt sowie Kompetenzen und Vertrauen im Umgang vermittelt werden.

Die ARD/ZDF-Offline-Studie 2004 [vgl. Gerhards & Mende 2004, 371ff.] hat ergeben, dass 83 % der Offliner ohne Computer auch definitiv keine Anschaffung in den nächsten zwölf Monate planen. Innerhalb der Gruppe derer, die zwar einen Computer besitzt bzw. dessen Anschaffung plant, haben 64 % kein Interesse an einem Internetzugang. Um die Nonliner vom Nutzen des Internets zu überzeugen, ist es erforderlich, die Motive dieser strikten Ablehnung herauszufinden.

Tendenziell lassen sich zwei Hauptgründe für die Nichtnutzung des Computers sowie des Internets ausmachen: einerseits wird von dem Medium kein hoher Nutzwert erwartet, andererseits wirkt die Komplexität des Mediums abschreckend. 93 % der Offliner halten die Informations- und Unterhaltungsangebote in den klassischen Medien für ausreichend, 85 % sind auf das Internet weder beruflich noch privat angewiesen. Im internationalen Vergleich verfügt Deutschland zusätzlich über relativ hohe Anschlussgebühren für einen Internetzugang [vgl. Initiative D^{21} 2000, 24]. Daher werden die Anschaffungs- und Unterhaltungskosten als nicht gerechtfertigt angesehen. Darüber hinaus traut sich gut ein Drittel der Nichtnutzer die Benutzung der Internets nicht zu bzw. könnte niemanden fragen, der den Einstieg erleichtern würde. Die Datenflut sowie die Begrifflichkeiten und Techniken, die sich rund um die Internetnutzung gebildet haben, schafft bei den Offlinern altersübergreifend ein Gefühl der Überforderung. Trotzdem glauben fast 90 % an die gleichwertige Etablierung des Internets neben den klassischen Medien.

Es gilt also, bei Kosten und Benutzerfreundlichkeit anzusetzen und entsprechende Hilfestellung zu bieten. Dies wird bestätigt durch die ARD/ZDF-Offline-Studie 2004, in der rund zwei Drittel der Offliner angaben, dass zusätzliche Informations- und Schulungsangebote das Internet interessanter machen würden. Zur besseren Orientierung sollte daher das bereits vorhandene Angebot zentral erfasst werden[170]. Zudem würde eine offizielle Zertifizierung der Kurse[171] als vertrauensbildende Maßnahme in deren Qualität dienen. Daneben ist der Ausbau der Online-Bereitstellung staatlicher Kernleistungen, wie z.B. administrative Behördengänge und interaktive Kommunikations- und Partizipationsfunktionen, erstrebenswert. Die Etablierung eines funktionsfähigen und benutzerfreundlichen ‚rundum'-Angebots lässt vermuten, dass das Vertrauen in den Staat als E-Government-Betreiber wächst. Gelingt die Ausweitung des E-Government-Systems auf E-Voting, kann davon ausgegangen werden, dass auch das Vertrauen in elektronische Wahlen steigt. Ferner sind insbesondere alltagsrelevante Bedürfnisse zu beachten. Die Angebote sollten auf die soziodemographischen Strukturen der Offliner zugeschnitten sein und die Vorteile des Internets (Zeitersparnis, ‚rund-um-die-Uhr-Erreichbarkeit' des öffentlichen Sektors) gegenüber der herkömmlichen Abwicklung von z.B. administrativen Behördengängen aufzeigen. In Bezug auf internetgestützte Wahlen sollten spezielle Kurse im Vorfeld der Wahl das Angebot ergänzen, um den sicheren Umgang mit dem Wahlsystem zu fördern und Berührungsängste mit dem Medium zu mindern.

5.2 Ausbau der Public Key Infrastruktur

Neben der Minderung der digitalen Spaltung setzt die Einführung des E-Votings den Ausbau der Public-Key-Infrastruktur voraus, um den Einsatz von chipkartenbasierten digitalen Signaturen zur Identifizierung und Authentifizierung der Wähler zu gewährleisten. Eine PKI nach den Bestimmungen des SigG und der SigV sichert den Nachweis der Urheberschaft digitaler Signaturen.

[170] Die ‚Stiftung Digitale Chancen' z.B. erstellt eine Datenbank der Zugangs- und Lernorte. Die Stiftung besteht seit 2002 und setzt sich aus Mitgliedern der Universität Bremen, AOL Deutschland, dem Beratungsunternehmen Accenture und der Burda Akademie zum 3. Jahrtausend zusammen. Hervorgegangen ist die Stiftung aus dem Projekt ‚Netzwerk Digitale Chancen', das im März 2001 an der Universität Bremen startete. Aufgabe war, im Auftrag des Bundesministeriums für Wirtschaft ein Informationssystem aufzubauen, das sich mit dem Problem der digitalen Spaltung befasst. Bis jetzt konnten jedoch lediglich 6.000 Einrichtungen verzeichnet werden.

[171] Möglich wäre eine unabhängige Prüfstelle, deren Zertifizierung dem Bürger als Orientierungshilfe im Angebot der Kurse dienen könnte (ähnlich wie die Stiftung Warentest bzw. TÜV).

Der gesetzeskonforme Einsatz digitaler Signaturen erfordert bei der Vergabe von Zertifikaten ein Netzwerk verschiedener Institutionen [vgl. Bertsch 2002, 23]. Neben den Zertifizierungsstellen[172], deren Aufgabe vor allem die Vergabe, Bereitstellung und Sperrung der Zertifikate ist, kontrolliert die Regulierungsbehörde für Telekommunikation und Post (RegTP) die Zertifizierungsstellen sowie die Durchsetzung der an die Betreiber gestellten rechtlichen Anforderungen nach dem SigG. Die Eignung der zur Erzeugung digitaler Signaturen eingesetzten Algorithmen wird vom Bundesamt für Sicherheit in der Informationstechnik festgestellt und jährlich geprüft. Der rechtliche Rahmen für den umfassenden Einsatz ist somit gegeben.

In der Praxis wird die PKI dennoch kaum genutzt, da ein unzureichendes Angebot an Kommunikations- und Transaktionsvorgängen, die Verwendung einer qualifizierten elektronischen Signatur mit Anbieter-Akkreditierung erfordern[173], besteht. Zur Förderung der Verbreitung der digitalen Signatur gründeten Staat und Wirtschaft 2003 das ‚Bündnis für elektronische Signaturen'[174]. Durch die Einbindung vorhandener Karteninfrastrukturen soll dem Bürger die Nutzung einer Vielzahl der Anwendungen im E-Commerce sowie im E-Government ermöglicht werden. Hierfür ist u.a. geplant, die Anfangsinvestition zu tragen, um einen möglichst großen Nutzerkreis zu gewinnen. Die Initiative ist zu begrüßen. Es ist jedoch zu bedenken, dass eine chipkartenbasierte digitale Signatur derzeit jährlich ca. 45 €[175] kostet. Diese Kosten würden sich erst bei umfassenden Einsatzmöglichkeiten im E-Commerce sowie im E-Government rentieren. Es ist daher zu vermuten, dass erst der Ausbau des Status' der chipkartenbasierten digitalen Signatur im Sinne eines virtuellen Repräsentanten des Bürgers das Interesse an der digitalen Signatur aufgrund der verbesserten Nutzungsmöglichkeiten steigert [vgl. Otten 2002, 85].

Interessant ist in diesem Zusammenhang das estnische Verfahren[176], das die elektronische Signatur in einem Personalausweis integriert. Dies lässt einerseits die Anschaffungskosten für die Bürger entfallen, andererseits bewirkt die hohe Verbreitung der digitalen Signatur ein weitreichendes Angebot an Einsatzmöglichkeiten sowohl im priva-

[172] Zu den Zertifizierungsstellen vgl. Kapitel 2.4.3.1.4.
[173] Zur Typologie vgl. Kapitel 2.4.3.1.4.
[174] Siehe http://www.signaturbuendnis.de (Verifizierungsdatum: 16.09.2005).
[175] Siehe http://www.deutschepost.de/dpag?check=yes&lang=de_DE&xmlFile=49577 (Verifizierungsdatum: 16.09.2005).
[176] Zu den estnischen Projekten vgl. Kapitel 3.3.

ten als auch im öffentlichen Sektor. Darüber hinaus fördert dies die wirtschaftliche Rentabilität. So würde die Verbreitung der digitalen Signatur sowie der Ausbau und die Kontrolle der Infrastruktur u.a. zu einer Aufgabe des öffentlichen Sektors und allein durch die hohe Verbreitung wirtschaftlich rentabel.

In Deutschland könnte eine derart weitreichende Einführung aus Datenschutzgründen auf Schwierigkeiten stoßen. Insbesondere in der Diskussion um ‚biometrische Reisepässe' wird die Schaffung eines ‚gläsernen Bürgers' kritisiert. Auch besteht die Befürchtung, der Staat könnte durch Kombination gesammelter Daten sogar die Wahlentscheidung eines jeden Bürgers ausmachen [vgl. Bittner 2005]. Dem kann entgegengehalten werden, dass bei entsprechender Architektur der Chipkarte die Anonymität des Karteninhabers gewährleistet werden kann [vgl. Otten 2002, 85].

5.3 Änderungsbedarf des Wahlrechts

Nach geltendem Recht können keine Internetwahlen durchgeführt werden. Zwar verbietet das BWG die Internetwahlen nicht explizit, die vorhandenen Vorschriften reichen jedoch als Rechtsgrundlage nicht aus [vgl. Karpen 2005, 60]. Die Bundeswahlgeräteverordnung[177] lässt grundsätzlich „mechanisch oder elektrisch betriebene einschließlich rechnergesteuerte Geräte" [§ 1 BWahlGV] zur Wahl zu; Wahlgeräte mit Netzanschluss fallen nicht darunter [vgl. Schreiber 2002, 512].

Die Einführung von Internetwahlen erfordert folglich eine Modifizierung der bestehenden sowie die Schaffung neuer Gesetze. Dies verlangt zunächst das Erstellen der Zulassungsbestimmungen für die im Wahlsystem eingesetzten Hard- und Softwarekomponenten. Da aus rechtlicher Sicht lediglich Rahmenbedingungen festgesetzt werden können, wären die technischen Details, die diesen gerecht werden, durch Experten zu beurteilen [vgl. Rüß 2002, 49]. Die Prüfung der Wahlgeräte erfolgt nach § 2 Absatz 2 BWahlGV durch die Physikalisch-Technische Bundesanstalt, die Zulassung durch das Bundesministerium des Innern. Eine derartige Regelung wäre auch für internetbasierte Wahlsysteme zu schaffen, sei es durch entsprechende Anwendung der BWahlGV oder durch Erlass einer gesonderten Verordnung für internetbasierte E-Voting-Systeme. Zusätzlich sollte die Zulässigkeit der Prüfung bzw. Zertifizierung durch private Dritte in Betracht gezogen werden.

[177] Die Bundeswahlgeräteverordnung wird im Folgenden als BWahlGV bezeichnet.

Von Bedeutung sind ferner eine Regelung zur Speicherung der Stimmen sowie die Gewährleistung einer Wahlprüfung nach Artikel 41 GG. Da § 10 BWG die Öffentlichkeit der Stimmauszählung verlangt, wäre auch beim E-Voting deren nachvollziehbare Gestaltung sicherzustellen [vgl. Bremke 2004, 108].

Die rechtlichen Rahmenbedingungen zum Ausbau der PKI sind mit dem SigG und der SigV gegeben, es bedarf jedoch einer Regelung zum Vergabemodus der chipkartenbasierten digitalen Signatur. Auch stellt sich die Frage nach der Kostentragung.

Bei Einführung der internetgestützten Fernwahl als Ausnahme zur Präsenzwahl wäre zudem über Kriterien für Hinderungsgründe ähnlich denen des § 25 Absatz 1 BWO zu entscheiden. Daneben ist es notwendig, den Wahlzeitraum festzulegen. Bei der internetbasierten Wahl im Wahllokal ergibt sich hierbei voraussichtlich kein Änderungsbedarf, im individuellen Bereich könnte die Fernwahl der Briefwahl als ‚Voraus-Wahl' gleichgesetzt, aber auch zur Förderung der ‚Gleichzeitigkeit der Wahl' [Kerpen 2005, 61] am eigentlichen Wahltag zugelassen werden. Bei einer internetgestützten Wahl im individuellen Bereich ist zusätzlich die Erstellung eines Anforderungsprofils an den Wählercomputer[178] erforderlich.

Jedenfalls ist die Digitalisierung der Wählerverzeichnisse vonnöten. Sollte die Einführung des E-Votings zu einer Reduzierung der Anzahl der Wahllokale führen, ist eine Anpassung des § 2 BWG bezüglich der Gliederung des Wahlgebiets sowie des § 3 BWG zur Einteilung der Wahlkreise erforderlich. Ferner wären auch die Aufgaben bzw. die Zusammensetzung der Wahlvorstände zur Umsetzung der digitalen Gewaltenteilung zu modifizieren. Einerseits sollten Anwesenheit und Zuständigkeiten von Experten geregelt werden, andererseits erfordert die Einführung der neuen Technologie Medienkompetenz auf Seiten des Wahlvorstandes [vgl. Kubicek & Wind 2002, 101]. Nicht zuletzt sollte die Schaffung einer Rechtsgrundlage für einen ‚Notfallplan' bedacht werden, die bei einem eventuellen Systemausfall das Vorgehen der Wahlvorstände festlegt, um die Rechtmäßigkeit der Wahl trotz technischer Probleme zu gewährleisten.

5.4 Einführungsmodelle des E-Votings

Die Einführung der politischen Internetwahl erfordert die Lösung einer Vielzahl von rechtlichen und organisatorischen Fragen, um die Einhaltung der demokratietheoreti-

[178] Unter diese Kriterien könnten z.B. die Rechnerleistung, Modell und Alter fallen. Falls kein Parallelsystem eingesetzt wird, würden darunter z.B. auch die Art und Version des Betriebsystems fallen.

schen sowie sicherheitstechnischen Grundsätze gewährleisten können. Mit gewissen Einschränkungen bezüglich des Grades der örtlichen Dezentralisierung sowie des Status' des E-Votings im Konzept der Stimmabgabe ist die Einführung des E-Votings möglich. Da die internetgestützte Wahl allenfalls als Ergänzung zur herkömmlichen Präsenz- und Briefwahl eingeführt werden könnte, ist die digitale Spaltung kein Hinderungsgrund, Internetwahlen innerhalb oder außerhalb des Wahllokals einzuführen [vgl. Hanßmann 2003, 190]. Somit ist die Frage nach dem Grad der örtlichen Dezentralisierung des Wahlvorgangs bezüglich der Gewährleistung der nach Artikel 38 GG festgelegten Wahlrechtsgrundsätze besonders interessant. Gleichzeitig müsste die Parlamentsebene, auf der E-Voting zunächst eingeführt würde, bedacht werden.

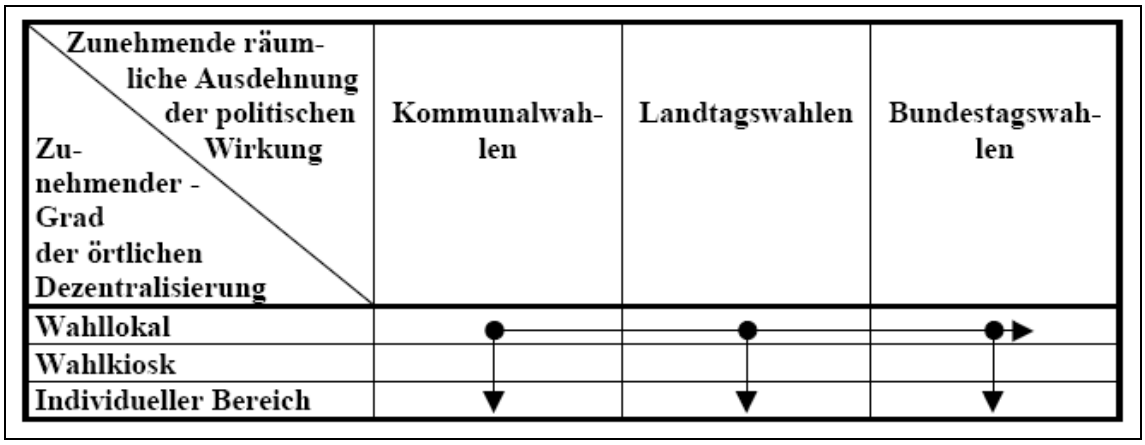

Abbildung 8: Einführungsebenen des E-Votings.

Bei einer möglichen Einführung des E-Votings scheint es angebracht, den Grad der örtlichen Dezentralisierung sowie die zunehmende räumliche Ausdehnung der politischen Wirkung stufenweise zu steigern[179]. Hierbei sollte die internetgestützte Präsenzwahl auf kommunaler Ebene als Ausgangspunkt dienen. Durch die gesicherte Umgebung im Wahllokal kann die eingesetzte Soft- und Hardware durch den Wahlvorstand kontrolliert werden. Des Weiteren betreffen Kommunalwahlen im Gegensatz zu einer Bundestagswahl einen relativ kleinen Teil der Bevölkerung; die Auswirkungen und Risiken einer politischen Wahl auf dieser Ebene sind somit zunächst auf ein vergleichsweise kleines Gebiet beschränkt. Zusätzlich ist der Organisationsaufwand überschaubar, so

[179] Dies entspricht auch dem Vorgehen in der Schweiz, die in vier Etappen vorgeht: elektronisches Abstimmen, elektronisches Wählen, elektronische Unterschriftensammlungen und elektronische Wahlvorschläge. Vgl.[Schweizerischer Bundesrat 2002, 673f.]. Die Empfehlungen der California Internet Voting Task Force, ein Zusammenschluss von Experten verschiedener Fachrichtungen zur Untersuchung der technischen und rechtlichen Möglichkeiten von Internetwahlen, sprechen sich ebenfalls für eine stufenweise Einführung aus. Vgl. [California Internet Voting Task Force 2000]. Vgl auch [Kubicek/Wind 2002], [Hanßmann 2003]. Kritisch [Will 2002].

dass die Ressourcen auf die Entwicklung überzeugender technischer Lösungen konzentriert werden könnten. Die erprobten und entwickelten Verfahren sollten nach erfolgreichen Testläufen auf kommunaler Ebene zunächst auf Länder- und später auf Bundesebene übertragen werden, so dass das Risikopotential für eine Bundestagswahl eingedämmt würde.

5.4.1 E-Voting im Wahllokal

Bei einer Internetwahl im Wahllokal könnten die Wähler durch eine Vernetzung der Wahllokale wahlkreisunabhängig ihre Stimme abgeben [vgl. Otten 2002, 92]. Die geheime Stimmabgabe in der Wahlkabine würde sich gemäß den äußeren Gegebenheiten im Wahllokal nicht von der herkömmlichen Präsenzwahl unterscheiden, da die öffentliche Kontrollmöglichkeit im Sinne einer Überprüfung der freien Ausübung des Wahlaktes gegeben ist. Der Teil der Briefwähler, der sich zwar außerhalb ihres Wahlkreises, jedoch innerhalb Deutschlands aufhält, könnte seine Stimme in jedem beliebigen Wahllokal abgeben; die erforderliche Medienkompetenz der betroffenen Wähler vorausgesetzt. Der stetig steigenden Zahl der Briefwähler würde so entgegengewirkt und die Briefwahl auf wirklich begründete Fälle wie Krankheit oder Aufenthalt im Ausland reduziert [vgl. Birkenmaier 2004, 123]. Gleichzeitig würde dem, aus der steigenden Briefwählerzahl abgeleiteten Interesse an einer flexibleren Stimmabgabe Rechnung getragen. Eine freizeitbedingte Mobilität fällt rechtlich nicht unter den nach § 25 BWO anerkannten Hinderungsgrund, verfassungsrechtlich spricht jedoch nichts gegen eine Stimmabgabe im Wahllokal außerhalb des Heimatwahlkreises [vgl. ebd.]. Aufgrund der Stimmabgabe am eigentlichen Wahltag entfiele bei dieser Variante die ‚Voraus-Wahl' und die Gleichzeitigkeit der Wahl würde gefördert.

Erfolgt die Identifizierung der Internetwähler durch den Einsatz digitaler Signaturen automatisch, ist aufgrund der Zeitersparnis eine größere Wahlkreiseinteilung gemäß § 12 Absatz 2 BWO denkbar. Die daraus resultierende Reduzierung der Anzahl der Wahllokale sowie des Aufwandes der administrativen Arbeit der Wahlhelfer könnte eine Kostensenkung bewirken. Zu beachten ist jedoch, dass der Grundsatz der Allgemeinheit der Wahl nicht durch längere Wege gefährdet würde[180]. Erfolgt die Identifizierung der Wähler auf herkömmliche Weise durch manuellen Abgleich der Wahlberechtigung mit

[180] Vgl. Kapitel 4.1 zum finanziellen Aufwand.

dem jeweiligen digitalisierten Wählerverzeichnis durch den Wahlvorstand, entfiele das Problem der mangelnden Verbreitung der chipkartenbasierten digitalen Signatur.

Schließlich wahrt diese Variante des E-Votings auch den Grundsatz der gleichen Wahl, da der technischen Zugang zum Internet im Wahllokal jedem Wähler offen steht [vgl. Forschungsgruppe Internetwahlen 2002, 26]. Besteht die Technik der Vernetzung, wäre es zudem denkbar, ‚mobile Wahllokale' an Punkten wie z.B. Krankenhäusern aufzustellen, deren Patienten andernfalls auf die Briefwahl, die zudem antragsbedürftig ist und daher einer Vorausplanung bedarf, angewiesen wären.

Bezüglich der sicherheitstechnischen Bedenken zur Einhaltung der freien, gleichen und geheimen Wahl ergeben sich bei der internetgestützte Präsenzwahl die wenigsten Bedenken [vgl. Forschungsgruppe Internetwahlen 2002, 83]. Im Vergleich zur Wahl im individuellen Bereich könnte mit relativ wenig Aufwand eine sichere Wahlumgebung geschaffen werden. Die Installation umfasst ausschließlich die erforderliche Wahlsoftware sowie einen Zugang zum Internet; andere Programme oder Komponenten sind nicht erforderlich. Eine gesicherte Verbindung zu den notwendigen Servern minimiert zusätzlich die Gefahren durch Malware, Spoofing und andere Sicherheitsrisiken.

5.4.2 E-Voting außerhalb des Wahllokals

Dem E-Voting außerhalb des Wahllokals ist nicht nur die Fernwahl von einem beliebigen Internetzugang zuzuordnen, sondern auch die Stimmabgabe von Wahlkiosken. In Wahlkiosken ist die technische Wahlumgebung zwar von staatlicher Seite zur Verfügung zu stellen, die Einhaltung der Wahlrechtsgrundsätze kann mangels Kontrollmöglichkeit jedoch nicht gewährleistet werden. Rechtlich ist diese Variante somit als Fern- und nicht als Präsenzwahl einzuordnen [vgl. Hanßmann 2003, 194]. Die Wahl im Wahlkiosk sowie die Wahl von einem beliebigen Internetanschluss ist somit nach geltendem Wahlrecht an eine vorherige Antragsstellung und Glaubhaftmachung eines anerkannten Hinderungsgrundes nach § 25 BWO gebunden.

Bei der Einführung des E-Votings als optionale Alternative im individuellen Bereich kann mit einem weiteren Anstieg der Fernwähler gerechnet werden. Somit steigt die Anzahl der Wähler, deren geheime Stimmabgabe nicht öffentlich zu garantieren ist [vgl. Buchstein 2000a, 900]. Der Ausnahmefall der Fernwahl im Sinne der Rechtssprechung

des BVerfG[181] ist hiermit nicht mehr gegeben. Die obligatorische Geheimwahl wandelt sich so für einen maßgeblichen Teil der Wähler in eine fakultative [vgl. Buchstein 2002, 65]. Voraussetzung für die Einführung einer Internetwahl im individuellen Bereich scheint ein erneutes Urteil des BVerfG bezüglich der Abwägung zwischen dem Wahlrechtsgrundsatz der geheimen und der allgemeinen Wahl[182].

Unter sicherheitstechnischen Aspekten gestaltet sich die Wahl von einem beliebigen Internetanschluss aufwendig. Hier kann nicht sichergestellt werden, dass private Computer frei von Malware und anderen Sicherheitsrisiken sind, die die freie, gleiche und geheime Wahl durch Ausspähen, Manipulieren, Vervielfältigen oder Löschen der Wahlstimme gefährden. Um diese Bedrohungen auszuschließen, müsste mithilfe eines von einer Live-CD[183] gestarteten Parallelsystems eine gesicherte Wahlumgebung geschaffen werden. Die hierfür erforderliche Konfiguration des Computers setzt eine grundlegende Medienkompetenz des Wählers voraus. Grundsätzlich sollte hierfür im Bedarfsfall Hilfestellung geboten werden. Zusätzlich ist die Beschaffung und Installation eines Kartenlesegerätes notwendig. Bereits eine internetgestützte Präsenzwahl ermöglicht eine heimatwahlkreis-unabhängige Wahl am Wahltag und wird so dem steigenden Interesse an flexibleren Wahlmöglichkeiten gerecht. Daher ist fraglich, ob dieser finanzielle und organisatorische Aufwand im Verhältnis zum erwarteten Nutzen des E-Votings im individuellen Bereich steht. Wird der einzige Vorteil dieser Variante in der Befriedigung der Bequemlichkeit des Wählers gesehen [vgl. Otten 2002, 83], wäre dies negativ zu bewerten. Bedenkt man jedoch z.B. Immobile und Auslandsdeutsche, denen der Zugang zur Wahl durch das E-Voting u.U. erleichtert werden würde, bietet die Variante im individuellen Bereich enorme Vorteile. So konnte bei der Bundestagswahl 2005 aufgrund verkürzter Fristen frühestens drei Wochen vor dem Wahltag mit der Versendung der Briefwahlunterlagen begonnen werden [vgl. Hahlen 2005]. Bei längeren Postwegen kann die rechtzeitige Rücksendung der Wahlbriefe nicht garantiert werden[184]. Einige Auslandsdeutsche werden somit de facto von ihrem Wahlrecht ausgeschlossen. Eine Stimmenübermittlung über das Internet könnte diesem Problem entgegenwirken.

[181] Siehe BVerfGE 21, 200 (204f.) und BVerfGE 59, 119 (124f., 126).
[182] Vgl. Kapitel 2.3.1 zur allgemeinen Wahl und Kapitel 2.3.5 zur geheimen Wahl.
[183] Vgl. Kapitel 2.4.3.4 zur Sicherheit des Clients.
[184] Siehe auch ‚Auslandsdeutschen droht Verlust des Wahlrechts durch vorgezogene Bundestagswahl' unter http://www.spiegel.de/spiegel/vorab/0,1518,368518,00.html (Verifizierungsdatum: 16.09.2005).

6 Resümee

Im Zuge der wachsenden Bemühungen der öffentlichen Verwaltungen in Deutschland, die Anwendungen des E-Governments zu realisieren (z.B. Initiative ‚Bund Online 2005'), stellt sich die Frage nach der Einbindung des Internets in den politischen Meinungs- und Willensbildungsprozess von Parteien, Wahlbevölkerung u.a.. Durch Interaktivität sowie nicht hierarchische Ordnung ermöglicht das Internet neue Wege zur Information, Kommunikation und Partizipation. Der Bürger kann unabhängig von den traditionellen Massenmedien sein Wissen erweitern und selbständig in den Willensbildungsprozess einbringen. Je mehr das Internet hierbei genutzt wird, desto stärker drängt sich die Frage auf, ob nicht auch das Internet bei politischen Wahlen eingesetzt werden kann oder sollte. Insbesondere angesichts sinkender Wahlbeteiligung und abnehmender Partizipationsbereitschaft verfügt das Internet über beachtliches kompensatorisches Potential.

Die offene Datenübertragung im Internet lässt die Durchführung von Wahlen zunächst problematisch erscheinen. Die in Kapitel 2.4 dargestellten Sicherheitsrisiken verdeutlichen den drohenden Verlust an Vertraulichkeit, Integrität und Authentizität der Wahlstimmen durch die Übermittlung im Internet sowie die nicht zu garantierende durchgehende Verfügbarkeit des Wahlsystems und heben die Gefahr für die verfassungsrechtlich normierten Wahlrechtsgrundsätze hervor. Um die freie, gleiche und geheime Wahl im Sinne des Artikels 38 Absatz 1 GG zu gewährleisten, sind die Identifizierung des Wählers sowie die Entkopplung der Wahlstimme von der Wähleridentität erforderlich. Gleichzeitig sind die Datenübermittlung vor dem Abhören und die Voten vor Manipulation, Löschung oder Vervielfältigung zu bewahren. Das gesamte Wahlsystem ist gegen externe Hacker-Angriffe und interne Manipulationsversuche, z.B. durch zugangsberechtigte Systemadministratoren oder Wahlhelfer, zu schützen. Durch den Einsatz kryptologischer Verfahren zur verschlüsselten Datenübertragung sowie zur Identifizierung und Authentifizierung des Wählers mithilfe digitaler Signaturen, einer permanenten technischen Systemüberwachung sowie der physischen und organisatorischen Trennung der unterschiedlichen Wahlserver (‚digitale Gewaltenteilung') kann ein komplexes Wahlverfahren, entsprechend dem in Kapitel 2.4.4 skizzierten exemplarischen technischen Ablaufs, entwickelt werden, das den sicherheitstechnischen Anforderungen einer politischen Wahl entspricht.

Für die Wahrung der Wahlrechtsgrundsätze ist jedoch nicht ausschließlich die Systemsicherheit, sondern auch der Grad der Dezentralisierung sowie der Status des E-Votings im Konzept der Stimmabgabe entscheidend (siehe Kapitel 2.2 Abbildung 1). Die ungleichen Zugangsmöglichkeiten zum Internet sowie der Umstand, dass die erforderliche Medienkompetenz nicht in der gesamten Bevölkerung vorausgesetzt werden kann, schließen die Einführung der Internetwahl als neue Regelform aus. Einer ausschließlichen Internetwahl im individuellen Bereich steht zusätzlich die Wahrung der freien und geheimen Stimmabgabe entgegen. Nach der Rechtsprechung des BVerfG, die zu den Verfassungsproblemen der in vielerlei Hinsicht mit dem E-Voting vergleichbaren Briefwahl ergangen ist, bleibt die Fernwahl eine Ausnahme zur Präsenzwahl und kommt allein bei Vorliegen eines anerkannten Hinderungsgrundes in Betracht. Die Fernwahl als neue Regelform würde die bisherige obligatorische Geheimwahl in eine fakultative umwandeln; dies ist nach geltendem Recht verfassungswidrig. Die Internetwahl als optionale Alternative erweist sich dagegen als konform mit den Wahlrechtsprinzipien und würde dem Grundsatz der Allgemeinheit der Wahl sogar in besonderem Maße entsprechen. Dies gilt auch für die internetbasierte Stimmabgabe im Wahllokal. Die Vernetzung der Wahllokale könnte zusätzlich der wachsenden Mobilität der Wähler Rechnung tragen, indem die Stimmabgabe unabhängig vom Heimatwahlkreis ermöglicht würde.

Die kritische Analyse der Ergebnisse sowohl nationaler und als auch internationaler Initiativen und Projekte aus Politik und Wirtschaft in Kapitel 3 konnte verdeutlichen, dass die Durchführung einer internetgestützten Stimmabgabe unter bestimmten Voraussetzungen möglich ist. Die Einführung einer Internetwahl in Deutschland bedarf zunächst der Schaffung eines rechtlichen Rahmens. Dies beinhaltet einerseits allgemeine Kriterien an die Verfassungskonformität des E-Voting-Systems hinsichtlich der technischen Gestaltung, andererseits sind Zuständigkeiten, Anforderungen und Kontrollinstanzen festzulegen, die das eingesetzte Wahlsystem prüfen und zertifizieren. Zusätzlich ist die Einbindung der Internetwahl in das geltende Wahlrecht erforderlich.

Dem Aufwand, diese normativen Voraussetzungen zu schaffen, stehen Rationalisierungspotentiale bezüglich der Kosten sowie des zeitlichen Ablaufs der Wahl und dem Feststellen der Ergebnisse gegenüber. Zudem könnte die Einbeziehung des politischen Willensbildungsprozesses im Vorfeld der Wahl in das Konzept des E-Votings der sinkenden Wahlbeteiligung sowie steigender ‚Politikverdrossenheit' entgegenwirken.

In Kapitel 4.3 wurde gezeigt, dass zivilgesellschaftliches und politisches Engagement durch eine sich gegenseitig verstärkende Wirkung verbunden sind. Durch den Ausbau der interaktiven Kommunikation, Information und Partizipation gerade auf lokaler Ebene können Probleme diskutiert werden, die für Bürger, aufgrund der direkten Betroffenheit, alltagsrelevant sind. Auch erste Online-Parteitage, bei denen Nicht-Parteimitgliedern die Möglichkeit zu Antragsstellung und Diskussion geboten wird, bieten eine neue Ebene der Transparenz für den Bürger. Das umfassende estnische Konzept zur Förderung des Einsatzes der Informationstechnologie im öffentlichen Sektor (vgl. Kapitel 3.3) bietet einen kostenlosen Internetzugang an öffentlichen Orten wie z.B. Bahnhöfen. Kombiniert mit der Einführung des digitalen Personalausweises, durch den jeder Bürger über eine elektronische Signatur verfügt, ist in Estland die Grundlage geschaffen, ab Oktober 2005 internetgestützte Wahlen als ergänzende Alternative anzubieten. Die gezielte Förderung der Medienkompetenz in der Bevölkerung sowie die Umstellung der Dienstleistungen des öffentlichen Sektors auf E-Government haben das Internet als Nutzungsgegenstand etabliert.

Werden die Sicherheitsanforderungen als grundsätzlich realisierbar eingestuft, ist dennoch davon auszugehen, dass die Einführung des E-Votings ein umfassendes Konzept und nicht lediglich eine Betrachtung der technischen Details erforderlich macht. Das Potential, das das Internet hinsichtlich demokratischer Prozesse besitzt, kann nur voll ausgeschöpft werden, wenn ein möglichst großer Teil der Bevölkerung das Internet nutzt. Die anderenfalls drohende Ausweitung der in Kapitel 5.1 analysierten digitalen Spaltung könnte negative Folgen für die Teilnahme der Bevölkerung am politischen Geschehen haben. Zwar wird auch das Internet nicht flächendeckend politisches Interesse wecken und zu einer qualifizierteren Informiertheit und Partizipation führen, jedoch gilt es, zumindest die Voraussetzungen für umfassende Beteiligungsmöglichkeiten zu schaffen. Aufgrund der elementaren Bedeutung, die dem Willensbildungsprozess in der Demokratie zukommt, sollte die Wahl nicht als reiner Akt der Stimmabgabe betrachtet werden. Die vorgelagerten Phasen der Kommunikation und Information müssten vielmehr explizit zu einer Steigerung des bürgerlichen Engagements, des politischen Interesses sowie des Vertrauens gegenüber Internet und Computern genutzt werden.

Die in Kapitel 5.4 entworfenen Einführungsmodelle verdeutlichen, dass es bei der Einführung von Internetwahlen zweckmäßig erscheint, den Grad der örtlichen Dezentralisierung stufenweise zu erhöhen, um die Anzahl der Fehlerquellen und die Sicherheitsri-

siken zu minimieren. Dient die internetbasierte Präsenzwahl dabei als Ausgangspunkt, können die Soft- und Hardwarekomponenten unter Kontrolle des Wahlvorstands stehen. Zusätzlich bietet diese Strategie neben der Gewöhnung an die Nutzung des Mediums und dem Aufbau von Vertrauen in die neue Technik auf Seiten der Wähler sowie der Wahlhelfer und Wahlvorstände auch die Möglichkeit, jeden Schritt zu evaluieren. Des Weiteren wäre es sinnvoll, Internetwahlen zunächst auf der unteren politischen Ebene durchzuführen. Eine derartige zweidimensionale Ausweitung (siehe Kapitel 5.4 Abbildung 8) basiert auf einer Nutzen-Risiko-Analyse, die auch einen Abbruch der Entwicklung beinhalten könnte, falls die nächste Stufe mit sicherheitstechnischen oder demokratietheoretischen Unwägbarkeiten verbunden ist, die außer Relation zu den erwarteten Vorteilen stehen. Zu beachten ist ferner, dass Wahlen auf höherer Parlamentsebene Kooperation zwischen verschiedenen Gebietskörperschaften erfordern. Die technischen Lösungen bedingen z.B. einheitliche Standards zur Digitalisierung der Wählerverzeichnisse. Diesen Ansatz verfolgt auch die Initiative ‚Bund Online 2005' der Bundesregierung, indem Behördendienstleistungen auf denselben Basiskomponenten und Standards beruhen.

Um in Deutschland Internetwahlen anbieten zu können, müsste, neben der Schaffung eines Rechtsrahmens sowie einer Sicherheitsinfrastruktur, ein Ausbau der administrativen Leistungen des E-Governments erfolgen. Die für E-Voting erforderlichen digitalen Signaturen werden sich nur durchsetzen, wenn vielseitige Einsatzmöglichkeiten bestehen. Die Einführung eines digitalen Personalausweises, der eine elektronische Signatur beinhaltet, ist in Deutschland jedoch nicht abzusehen. Daher scheinen die jährlichen Kosten für den Bürger nur vertretbar, wenn sich die chipkartenbasierte elektronische Signatur zu einem virtuellen Repräsentanten des Bürgers für Kommunikations- und Transaktionsvorgänge im Internet wandelt. Hat der Bürger einen konkreten Nutzen, steigt die Wahrscheinlichkeit der Etablierung der digitalen Signatur ebenso wie die Bereitschaft, dem Internet als Medium für Wahlen zu vertrauen. Dies ist grundlegende Voraussetzung für die Akzeptanz des neuen Wahlmodus'. Die Einführung des E-Votings kann daher nicht lediglich als eine rein technische Bereicherung eines im Übrigen unveränderten Wahlsystems gesehen werden; sie ist vielmehr Teil eines umfassenden internetgestützten Kommunikations- und Transaktionskonzeptes, zu dem die Anwendungen des E-Governments und des E-Commerce gleichermaßen gehören.

Literaturverzeichnis

Ahlert, Christian [2003]:

Weltweite Wahlen im Internet – Möglichkeiten und Grenzen transnationaler Demokratie. Campus Verlag: Frankfurt a.M..

Alvarez, R. Michael & Hall, Thad E. [2004]:

Point, Click and Vote - The Future of Internet Voting. The Brookings Institution: Washington D.C..

Aschenbach, Astrid [1999]:

Datenschutz und Datensicherheit im Internet – Verantwortung und Kontrolle. Art & Communication: Hamburg.

Baldersheim, Harald & Kersting, Norbert (Hrsg.) [2004]:

Electric Voting and Democracy - A comparative Analysis. Palgrave Macmillan: New York.

Barber, Benjamin R. [1998]:

Wie demokratisch ist das Internet? - Technologie als Spiegel kommerzieller Interessen. In: Leggewie & Maar [1998], S. 120-133.

Bauer, Harald & Gora, Walter (Hrsg.) [2001]:

Virtuelle Organisation im Zeitalter von E-Business und E-Government - Einblicke und Ausblicke. Springer-Verlag: Berlin und Heidelberg.

Bertelsmann Stiftung [2001]:

Balanced E-Governemnt – Elektronisches Regieren zwischen administrativer Effizienz und bürgernaher Demokratie. www.begix.de. (Verifizierungsdatum: 16.09.2005).

Bertelsmann Stiftung & Forschungsgruppe Wahlen [2004]:

Politische Partizipation in Deutschland. Ergebnisse einer repräsentativen Umfrage. Bundeszentrale für politische Bildung: Bonn.

Bertsch, Andreas [2002]:

Digitale Signaturen. Springer-Verlag: Berlin und Heidelberg.

Beutelspacher, Albrecht [1991]:

Kryptologie. Friedr. Vieweg & Sohn Verlagsgesellschaft: Braunschweig.

Bieber, Christoph [2002]:

'Elektronische' oder 'interaktive' Demokratie?. In: Kritische Justiz 35, S. 180-196. Nomos Verlaggesellschaft: Baden-Baden.

Bieber, Christoph & Hebecker, Eike [1998]:

Internet und soziale Bewegungen - Der Studentenstreik als Fallbeispiel. In: Gellner & Korff [1998], S. 171- 177.

Birkenmaier, Philipp [2004]:

E-Democracy - Der Wandel der Demokratie durch das Internet. Rhombos-Verlag: Berlin.

Bittner, Jochen [2005]:

Denn sie wissen, was wir tun. http://www.zeit.de/2005/10/Biometrie?page=all. (Verifizierungsdatum: 16.09.2005).

Braun, Nadja [2004]:

E-Voting – Switzerland's Projects and their Legal Framework in a European Context. In: Krimmer & Prosser [2004], S. 43-52.

Bremke, Nils [2004]:

Internetwahlen – Eine Analyse einer Wahlverfahrensergänzung für das 21. Jahrhundert unter besonderer Berücksichtigung rechtlicher Anforderungen. In: Landes- und Kommunalverwaltung. Verwaltungsrechtzeitschrift für die Länder Berlin, Brandenburg, Mecklenburg-Vorpommern, Thüringen, Sachesen und Sachsen-Anhalt 2004, Heft 3, S. 102- 109. Beck Juristischer Verlag: München.

Brettschneider, Frank & Deth, Jan van & Roller, Edeltraud [2002]:

Das Ende der politischen Sozialstruktur?. Leske + Budrich: Opladen.

Brockhaus [2003]:

Computer und Informationstechnologie. F.A. Brockhaus: Leipzig, Mannheim.

Buchmann, Johannes [2004]:

Einführung in die Kryptographie. Springer-Verlag: Berlin.

Buchstein, Hubertus [2000a]:

Briefwahl, Onlinewahl und der Grundsatz der geheimen Stimmabgabe. In: Zeitschrift für Parlamentsfragen Heft 4/2000, S.886-902. Westdeutscher Verlag: Wiesbaden.

Buchstein, Hubertus [2000b]:

Öffentliche und geheime Stimmabgabe - Eine wahlrechtshistorische und ideengeschichtliche Studie. Nomos Verlagsgesellschaft: Baden-Baden.

Buchstein, Hubertus [2002]:

Online-Wahlen und das Wahlgeheimnis. In: Buchstein & Neymanns [2002], S. 51-70.

Buchstein, Hubertus & Neymanns, Harald (Hrsg.) [2002]:

Online-Wahlen. Leske + Budrich: Opladen.

Bundesamt für Sicherheit in der Informationstechnik [2005]:

E-Government-Handbuch – Chefsache. E-Government-Leitfaden für Behördenleiter. http://www.bsi.bund.de/fachthem/egov/6.htm. (Verifizierungsdatum: 16.09.2005).

California Internet Voting Task Force [2000]:

A report on the feasibility of internet voting. http://www.ss.ca.gov/executive/ivote/final_report.pdf. (Verifizierungsdatum: 16.09.2005).

Chapman, D. Brent & Zwicky, Elizabeth D. [1996]:

Einrichten von Internet- Firewalls. O´Reilly: Köln.

Chaum, David [1981]:

Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms. Communication of the ACM Vol. 24 Nr.2.

Chaum, David [1982]:

Blind Signatures for Untraceable Payments. Proceedings of Crypto '82, S. 199-203. Plenum Press.

Cheswick, William R. & Bellovin, Steven M. [1996]:

Firewalls und Sicherheit im Internet. Addison-Wesley: Bonn.

Clemens, Detlev [1999]:

Netz-Kampagnen. Parteien und politische Informationslotsen in den Internet-Wahlkämpfen 1998 in Deutschland und den USA. In: Kamps [1999], S. 153-174.

Der Bundeswahlleiter [2003]:

Wahl zum 15.Deutschen Bundestag - Ergebnisse der Repräsentativen Wahlstatistik. Statistisches Bundesamt: Wiesbaden.

Der Bundeswahlleiter [2005]:

Wahlkostenerstattung. http://www.bundeswahlleiter.de/wahlen/abc/d/tw2.htm. (Verifizierungsdatum: 16.09.2005).

Donath, Matthias [2001]:

Demokratie und Internet - Neue Modelle der Bürgerbeteiligung an der Kommunalpolitik- Beispiele aus den USA. Campus Verlag: Frankfurt a.M..

Donges, Patrick & Jarren, Ottfried [1999]:

Politische Öffentlichkeit durch Netzkommunikation?. In: Kamps [1999], S. 85-108.

Egloff, Daniel [2002]:

Digitale Demokratie - Mythos oder Realität?. Westdeutscher Verlag: Wiesbaden.

Eimeren, Birgit van & Gerhard, Heinz & Frees, Beate [2004]:

Internetverbreitung in Deutschland: Potenzial vorerst ausgeschöpft? - ARD/ZDF Online Studie. In: Media Perspektiven 08/2004, S.350-370. http://www.ard-werbung.de/showfile.phtml/eimeren_gerhard_frees_8-2004.pdf?foid=12150. (Verifizierungsdatum: 16.09.2005).

Ellermann, Silvia [2004]:

Abschlussbericht zu dem Arbeitspaket 5.1. Analyse/Bewertung zur Akzeptanz. http://www.internetwahlen.de. (Verifizierungsdatum: 16.09.2005).

Engels, Dietrich [2004]:

Armut, soziale Ausgrenzung und Teilhabe an Politik und Gesellschaft. Institut für Sozialforschung und Gesellschaftspolitik: Köln.

Europarat [2004]:

Legal, operational and technical standards for E-Voting. Council of Europe Publishing: Strasburg.

Ewert, Burkhard & Faslic, Nermin & Kollbeck, Johannes [2003]:

E-Demokratie - Stand, Chancen und Risiken. In: Schulzki-Haddouti [2003], S. 227-260.

Fazlic, Nermin & Kollbeck, Johannes & Tauss, Jörg [2001]:

e-Recht und e-Demokratie - Die Modernisierung des Informationsrechts als Reformprojekt zur elektronischen Demokratie. In: Zeitschrift für Gesetzgebung 2001, S. 231-245. C. F. Müller Verlag: Heidelberg.

Federrath, Hannes (Hrsg.) [2005]:

Sicherheit 2005 - Sicherheit- Schutz und Zuverlässigkeit. Gesellschaft für Informatik: Bonn.

Federrath, Hannes & Berthold, Oliver & Köhntopp, Marit & Köpsell, Stefan [2000]:

Tarnkappe für das Internet – Verfahren zur anonymen und unbeobachteten Kommunikation. In: c't 16/2000, S. 148-158. Heise Zeitschriften Verlag: Hannover.

Feltz, Ferdinand & Oberweis, Andreas & Otjacques, Benoit (Hrsg.) [2004]:

EMISA 2004 - Informationssysteme im E-Business und E-Government. Gesellschaft für Informatik: Bonn.

Forschungsgruppe Internetwahlen [2000]:

Zweiter Zwischenbericht zum Projekt ‚Strategische Initiative: Wahlen im Internet' nach Abschluss der Wahlen zum Studierendenparlament der UOS am 2.Februar 2000. http://www.wahlkreis300.net/fgiw/uploader/data/stupa.pdf. (Verifizierungsdatum: 16.09.2005).

Forschungsgruppe Internetwahlen [2002]:

i-vote Report - Chancen, Möglichkeiten und Gefahren der Internetwahl. Universität Osnabrück. http://www.wahlkreis300.net/fgiw/uploader/data/Kurzfassung.pdf. (Verifizierungsdatum: 16.09.2005).

Fuhrberg, Kai [2000]:

Internet-Sicherheit - Browser, Firewalls und Verschlüsselung. Carl Hanser Verlag: München.

Gehrke, Gernot & Tekster, Thomas [2004a]:

Zwischen digitaler Teilung und Integration: Neue Befunde zum Stand der Nichtnutzung von Internet und Online-Diensten. Zum Hintergrund der Debatte um Teilung und Integration. http://www.digitale-teilung.de/doc/analyse/digitale-ti_zum_hintergrund_der_debatte_um_teilung_und_integration.pdf. (Verifizierungsdatum: 16.09.2005).

Gehrke, Gernot & Tekster, Thomas [2004b]:

Zwischen digitaler Teilung und Integration: Neue Befunde zum Stand der Nichtnutzung von Internet und Online-Diensten. Faktoren der Nichtnutzung – Motive und Gründe. http://www.digitale-teilung.de/doc/analyse/digitale-ti_faktoren_der_nichtnutzung.pdf. (Verifizierungsdatum: 16.09.2005).

Geis, Ivo [1999]:

Rechtsaspekte des elektronischen Geschäftsverkehrs - Auf dem Weg zur Informationsgesellschaft, Kryptologietechnologien: Digitale Signatur und Verschlüsselung, Rechtliche Rahmenbedingungen. AWV-Eigenverlag: Eschborn.

Gellner, Winand & Korff, Fritz von (Hrsg.) [1998]:

Demokratie und Internet. Nomos Verlagsgesellschaft: Baden-Baden.

Gerhards, Maria & Mende, Annette [2004]:

Offliner 2004: Anpassungsdruck steigt, Zugangsbarrieren bleiben bestehen. – ARD/ZDF Offline-Studie. In: Media Perspektiven 08/2004, S. 371-385. http://www.ard-werbung.de/showfile.phtml/gerhards_mende_8-2004.pdf?foid=12151. (Verifizierungsdatum: 16.09.2005).

Gora, Walther & Krampert, Thomas (Hrsg.) [2003]:

Handbuch IT-Sicherheit - Strategien, Grundlagen und Projekte. Addison-Wesley Verlag: München.

Hahlen, Johann [2005]:

Ablauf der Antragsfrist für wahlberechtigte Auslandsdeutsche zur Bundestagswahl 2005. http://www.bundeswahlleiter.de/wahlen/pm-wahl-16-dbt/pd120212.htm. (Verifizierungsdatum: 16.09.2005).

Hanßmann, Annika [2003]:

Möglichkeiten und Grenzen von Internetwahlen. Nomos Verlagsgesellschaft: Baden-Baden.

Hebecker, Eike [2002]:

Experimentieren für den Ernstfall - Der Online-Wahlkampf 2002. http://www.bpb.de/publikationen/F9V8FD,2,0,Experimentieren_f%FCr_den_Ernstfall_Der_OnlineWahlkampf_2002.html#art2. (Verifizierungsdatum: 16.09.2005).

Hesse, Konrad [1995]:

Grundzüge des Verfassungsrechts der Bundesrepublik Deutschland. C.F. Müller Verlag: Bonn.

Hill, Hermann [2002]:

Electronic Government - Strategie zur Modernisierung von Staat und Verwaltung. Bundeszentrale für politische Bildung: Bonn.

Hoecker, Beate [2002]:

Mehr Demokratie via Internet? - Die Potenziale der digitalen Technik auf dem empirischen Prüfstand. Bundeszentrale für politische Bildung: Bonn.

Hörisch, Jochen [2001]:

Der Sinn und die Sinne - Eine Geschichte der Medien. Eichborn Verlag: Frankfurt a.M..

Horster, Patrick (Hrsg.) [1995]:

Trust Center – Grundlagen, rechtliche Aspekte, Standardisierung, Realisierung. Vieweg Verlagsgesellschaft: Braunschweig und Wiesbaden.

Initiative D ^{21} [2000]:

Digitale Spaltung in Deutschland. Ausgangssituation, internationaler Vergleich, Handlungsempfehlungen.
http://www.initiatived21.de/druck/news/publikationen2000/doc/5_1053497463.pdf. (Verifizierungsdatum: 16.09.2005).

Initiative D ^{21} [2004]:

(N)Onliner Atlas 2004. Eine Topographie des digitalen Grabens durch Deutschland.
http://www.nonliner-atlas.de/pdf/NONLINER-Atlas2004_TNS_Emnid_InitiativeD21.pdf. (Verifizierungsdatum: 16.09.2005).

Initiative eParticipation [2004]:

Elektronische Bürgerbeteiligung in deutschen Großstädten 2004 - Website-Ranking.
http://www.initiative-eparticipation.de/studie_eparticipation.pdf. (Verifizierungsdatum: 16.09.2005).

Jansen, Stephan A. & Priddat, Birger P. [2001]:

Electronic Government - Neue Potentiale für einen modernen Staat. Klett-Cotta: Stuttgart.

Kamps, Klaus (Hrsg.) [1999]:

Elektronische Demokratie? - Perspektiven politischer Partizipation. Westdeutscher Verlag: Opladen.

Kamps, Klaus [2001]:

Politische Partizipation im Internet - Von der repräsentativen Demokratie zur 'Cyberdemocracy'. In: Koziol [2001], S. 26-35.

Karpen, Ulrich [2005]:

Elektronische Wahlen? - Einige verfassungsrechtliche Fragen. Nomos Verlagsgesellschaft: Baden-Baden.

Kelter, Harald & Koob, Frank & Ullmann, Markus [2001]:

Anonyme Online-Wahlen - Lösungsansätze für die Realisierung von Online-Wahlen. In: Datenschutz und Datensicherheit (DuD) 11/2001. Band 25, S. 643-647. Vieweg Verlag/GWV Fachverlage GmbH: Wiesbaden.

Kersting, Norbert [2004]:

Online-Wahlen im internationalen Vergleich. Bundeszentrale für politische Bildung: Bonn.

Kesdogan, Dogan & Rattay, Oliver [2005]:

Sicherheitsbewertung von Anonymisierungsverfahren im World Wide Web. In: Federrath [2005], S. 233-244.

Klein, Ansgar & Schmalz-Bruns, Rainer [1997]:

Politische Beteiligung und Bürgerengagement in Deutschland - Möglichkeiten und Grenzen. Nomos Verlagsgesellschaft: Baden-Baden.

Kleinsteuber, Hans J. [1999]:

Politik und Medienrevolution - Politikrelevante Aspekte der Kommunikationstechnik. In: Kamps [1999], S.39- 62.

Kloth, Hans Michael [2000]:

Vom 'Zettelfalten' zum freien Wählen - Die Demokratisierung der DDR 1989/90 und die 'Wahlfrage'. Ch. Links Verlag: Berlin.

Koch, Achim & Wasmer, Martina & Schmidt, Peter (Hrsg.) [2001]:

Politische Partizipation in der Bundesrepublik Deutschland - Empirische Befunde und theoretische Erklärungen. Leske + Budrich: Opladen.

Koenen, Andrea & Konert, Bertram [2004]:

Exkurs digitale Integration: Zur Notwendigkeit einer Definitionserweiterung. http://www.digitale-teilung.de/doc/analyse/digitale-ti_exkurs_digitale_integration.pdf. (Verifizierungsdatum: 16.09.2005).

Korff, Fritz von [1999]:

Kommunale Demokratie und das Internet. In: Kamps [1999], S. 191-208.

Korte, Karl-Rudolf [2003]:

Wahlen in der Bundesrepublik Deutschland. Bundeszentrale für politische Bildung: Bonn.

Koziol, Klaus [2001]:

E-Demokratie = Ende der Demokratie. Forum Medienethik, H.2001/1. KoPäd-Verlag: München.

Krempl, Stefan [2005]:

Bundesrat gibt grünes Licht für Informationsfreiheitsgesetz. http://www.heise.de/newsticker/meldung/61509. (Verifizierungsdatum: 16.09.2005).

Krimmer, Robert & Prosser, Alexander (Hrsg.) [2004]:

Electronoc Voting in Europe - Technology, Law, Politics and Society. Gesellschaft für Informatik: Bonn.

Kubicek, Herbert & Wind, Martin [2002]:

Bundestagswahl per Computer?. In: Buchstein & Neymanns [2002], S. 91-112.

Kuhlen, Rainer [1999]:

Die Konsequenzen von Informationsassistenten. Was bedeutet informationelle Autonomie oder wie kann Vertrauen in elektronische Dienste in offenen Informationsmärkten gesichert werden?. Suhrkamp Verlag: Frankfurt a.M..

Lange, Nico [2002]:

Click'n'Vote - Erste Erfahrungen mit Online-Wahlen. In: Buchstein & Neymanns [2002], S. 127-144.

LDS Brandenburg [2002]:

Abschlussbericht zur Online-Wahl im LDS Brandenburg. http://www.wahlkreis300.net/fgiw/uploader/data/LDS2000.pdf. (Verifizierungsdatum: 16.09.2005).

Leder, Martin [2002]:

Der Einsatz von Wahlgeräten und seine Auswirkungen auf die Amtlichkeit und Öffentlichkeit von Wahlen. Die Öffentliche Verwaltung, 55.Jahrgang. S.648-655. Kohlhammer: Stuttgart.

Lederer, Andreas [2003]:

eVoting Premiere in Österreich. http://www.politik-digital.de/edemocracy/evoting/oesterreich.shtml. (Verifizierungsdatum: 16.09.2005).

Leggewie, Claus [1998]:

Demokratie auf der Datenautobahn - Wie weit geht die Zivilisierung des Cyberspace? In: Leggewie & Maar [1998], S. 15-51.

Leggewie, Claus & Maar, Christa (Hrsg.) [1998]:

Internet und Politik - Von der Zuschauer- zur Beteiligungsdemokratie. Bollmann Verlag: Köln.

Leib, Volker [1998]:

Wissenschaftsnetze und Bürgernetze - Vom selbstgesteuerten Internet zur elektronischen Demokratie?. In: Gellner & Korff [1998], S. 81-94.

L'Etat de Genève [2005]:

E-Voting. http://www.geneve.ch/evoting/welcome.asp. (Verifizierungsdatum: 16.09.2005).

Losse, Bernd [2000]:

Abschied vom Kuschelsofa. In: Wirtschaftswoche Nr. 25 vom 15.06.2000, S. 34.

Lührs, Rolf [2004]:

Elektronische Demokratie 2004. http://www.politik-digital.de/edemocracy/netzkampagnen/elektronische_demokratie2004.shtml. (Verifizierungsdatum: 16.09.2005).

Maaten, Epp [2004]:

Towards remote E-Voting – Estonian case. In: Krimmer & Prosser [2004], S. 83-100.

Macintosh, Ann & Xenakis, Alexandros [2004]:

The UK deployment of the e-electoral register. In: Krimmer & Prosser [2004], S. 143-152.

Marr, Mirko [2005]:

Internetzugang und politische Informiertheit. Zur digitalen Spaltung der Gesellschaft. UVK Verlagsgesellschaft: Konstanz.

Marschall, Stefan [1998]:

Netzöffentlichkeit - eine demokratische Alternative?. In: Gellner & Korff [1998], S. 43-54.

Meier-Walser, Reinhard C. & Harth, Thilo (Hrsg.) [2001]:

Politikwelt Internet - Neue demokratische Beteiligungschancen mit dem Internet?. Olzog Verlag GmbH: München.

Meyer, Thomas [2001]:

Mediokratie - Die Kolonisierung der Politik durch die Medien. Suhrkamp: Frankfurt a. M..

Michels, Markus [1996]:

Kryptologische Aspekte digitaler Signaturen und elektronischer Wahlen. Shaker Verlag: Aachen.

Müller, Günter & Reichenbach, Martin (Hrsg.) [2001]:

Sicherheitskonzepte für das Internet. Springer-Verlag: Berlin und Heidelberg.

Müntefering, Franz [2004]:

Entwurf eines Gesetzes zur Regelung des Zugangs zu Informationen des Bundes - Informationsfreiheitsgesetz (IFG); Drucksache 15/4493 vom 14.12.2004. Deutscher Bundestag: Berlin.

Narusberg, Tea [2004]:

Tiger-Online: Estland. http://www.politik-digital.de/egovernment/international/estland2.shtml. (Verifizierungsdatum: 16.09.2005).

Neymanns, Harald [2002a]:

Be creative! Online-Wahlen und der Verlust der Wahlsymbole. http://www.politik-digital.de/edemocracy/evoting/creativ.shtml. (Verifizierungsdatum: 16.09.2005).

Neymanns, Harald [2002b]:

Die Wahl der Symbole - Politische und demokratietheoretische Fragen zu Online-Wahlen. In: Buchstein & Neymanns [2002], S. 23-37.

Niedermayer, Oskar [2001]:

Bürger und Politik - Politische Orientierungen und Verhaltensweisen der Deutschen - Eine Einführung. Westdeutscher Verlag: Wiesbaden.

N.N. [2002a]:

Erstmals elektronische Briefwahlanträge bei Bundeswahl. http://www.heise.de/newsticker/meldung/29553. (Verifizierungsdatum: 16.09.2005).

N.N. [2002b]:

Wählen auf Knopfdruck. http://www.wdr.de/themen/wahl2002/aktuell/wahlapparate.jhtml. (Verifizierungsdatum: 16.09.2005).

N.N. [2003]:

The Estonian ID Card and Digital Signature Concept – Principles and Solutions. http://www.id.ee/pages.php/03031002,408. (Verifizierungsdatum: 16.09.2005).

Nohlen, Dieter [2004]:

Wahlrecht und Parteiensystem. Leske + Budrich: Opladen.

Nusser, Stefan [1998]:

Sicherheitskonzepte im WWW. Springer-Verlag: Berlin und Heidelberg.

Oostveen, Anne-Marie & van den Besselaar, Peter [2004]:

Security as belief. User's perceptions on the security of electronic voting systems. In: Krimmer & Prosser [2004], S. 73-82.

Otten, Dieter [1998]:

Mehr Demokratie im Internet. Abschlussbericht zum Projekt ‚Wahlkreis 329'. http://www.wahlkreis300.net//fgiw/uploader/data/WK329-Report.pdf. (Verifizierungsdatum: 16.09.2005).

Otten, Dieter [2002]:

Modernisierung der Präsenzwahl durch das Internet. In: Buchstein & Neymanns [2002], S. 71-90.

Otten, Dieter & Küntzler, Jürgen [2002]:

Über die Herstellung von Anonymität bei elektronischen Wahlen. http://www.forschungsprojekt-wien.de/pdf/2003_05_anonymitaet_otten_DuD.pdf. (Verifizierungsdatum: 16.09.2005).

Philippsen, Michael [2002]:

Internetwahlen - Demokratische Wahlen über das Internet? In: Informatik-Spektrum 18. April 2002, S. 138-150. Springer-Verlag: Berlin und Heidelberg.

Physikalisch-Technische Bundesanstalt Braunschweig und Berlin [2004]:

Online-Wahlsysteme für nicht-parlamentarische Wahlen – Anforderungskatalog. Laborbericht PTB: Berlin.

Projekt ESI [2001]:

Erfahrungsbericht zur Internet-Testwahl – Landratswahl des Landkreises Marburg-Biedenkopf am 16.September 2001. http://www.wahlen.hessen.de/internetwahl.doc. (Verifizierungsdatum: 16.09.2005).

Puppe, Christoph & Maier, Jörn [2005]:

Von allen Seiten - Maßnahmen gegen Distributed-Denial-of-Service-Angriffe. In: ix-Magazin für professionelle Informationstechnik 04/2005, S. 107-112. Heise Zeitschriften Verlag: Hannover.

Rechenberg, Peter [2000]:

Was ist Informatik? Eine allgemeine Einführung. Carl Hanser Verlag: München.

Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates [1999]:

Über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen. Amtsblatt der Europäischen Gemeinschaften.

Rötzer, Florian [2000]:

E-Commerce Websites lahmgelegt - Nach Yahoo waren jetzt Ebay, Buy, Amazon und CNN das Ziel von koordinierten Angriffen.
http://www.heise.de/tp/r4/artikel/5/5766/1.html. (Verifizierungsdatum: 16.09.2005).

Roth, Roland [1997]:

Die Kommune als Ort der Bürgerbeteiligung. In: Klein & Schmalz-Bruns [1997], S.404-447.

Rüß, Oliver [2002]:

Rechtliche Voraussetzungen und Grenzen von Online-Wahlen. In: Buchstein & Neymanns [2002], S. 39-50.

Schabedoth, Eva & Schrott, Peter & Voltmer, Katrin [1995]:

Individuelle Teilnahme an politischer Kommunikation - Zur Bedeutung von interpersonaler und massenmedialer Kommunikation im Prozess der deutschen Wiedervereinigung. Westdeutscher Verlag: Opladen.

Schily, Otto [2001]:

Politische Partizipation in der Informationsgesellschaft; Rede beim Kongress "Internet - eine Chance für die Demokratie?. 03.Mai 2001. Berlin.

Schliesky, Utz [1999]:

Die Weiterentwicklung von Bürgerbegehren und Bürgerentscheid. In: Zeitschrift für Gesetzgebung 1999, S. 91-122. C. F. Müller Verlag: Heidelberg.

Schmitz, Christian [2002]:

Ein Netz voller Scheren, Barrieren und Chancen. Einfach für alle - Aktion Mensch. www.einfach-fuer-alle.de/artikel/barrieren/. (Verifizierungsdatum: 16.09.2005).

Schneier, Bruce [2000]:

Secrets & Lies - IT-Sicherheit in einer vernetzten Welt. dpunkt. Verlag: Heidelberg.

Schoch, Friedrich [2002]:

Informationsfreiheitsgesetz für die Bundesrepublik Deutschland. In: Die Verwaltung 35, S. 149-175. Duncker und Humblot: Berlin.

Schreiber, Wolfgang [2002]:

Handbuch des Wahlrechts zum Deutschen Bundestag – Kommentar zu Bundeswahlgesetz. Carl Heymanns Verlag KG: Köln.

Schulzki-Haddouti, Christiane (Hrsg.) [2003]:

Bürgerrechte im Netz. Bundeszentrale für politische Bildung: Bonn.

Schwartzenberg, Gitta v. & Geiert, Constanze [2002]:

Grundlagen und Daten der Wahl
zum 15. Deutschen Bundestag am 22. September 2002.
http://www.bundeswahlleiter.de/wahlen/download/wahlwista.pdf. (Verifizierungsdatum: 16.09.2005).

Schweizerische Bundeskanzlei [2004]:

Der Vote électronique in der Pilotphase. Zwischenbericht. http://www.admin.ch/ch/d/egov/ve/dokumente/Zwischenbericht.pdf. (Verifizierungsdatum: 16.09.2005).

Schweizerischer Bundesrat [2002]:

Bericht über den Vote électronique - Chancen, Risiken und Machbarkeit elektronischer Ausübung politischer Rechte. http://www.admin.ch/ch/d/ff/2002/645.pdf. (Verifizierungsdatum: 16.09.2005).

Segler, Daland [2005]:

Augenhöhe als Siegesbeweis? Nur Gewinner beim "TV-Duell". http://www.fr-aktu-ell.de/ressorts/kultur_und_medien/medien/?sid=19ffe4e75f4efe3923aa19ce05c1d626&cnt=721860. (Verifizierungsdatum: 16.09.2005).

Simonson, Julia [2003]:

Integration in freiwilligen Vereinigungen und politische Partizipation - Empirische Analysen auf Basis der ALLBUS-Daten. Universität Bremen: Bremen. http://www.sozialforschung.uni-bremen.de/integ1.pdf. (Verifizierungsdatum: 16.09.2005).

Statistisches Bundesamt [2004]:

Datenreport 2004 - Daten und Fakten über die Bundesrepublik Deutschland. Bundeszentrale für politische Bildung: Bonn. http://www.destatis.de/datenreport/d_datend.htm. (Verifizierungsdatum: 16.09.2005).

Stadt Braunschweig [2000]:

Wahlkostenerstattung in deutschen Städten. Untersuchung für die Projektgruppe ‚Wahlkosten' des Statistischen Ausschusses des Deutschen Städtetages.

Stadt Fellbach [2001]:

Jugendgemeinderatswahl in Fellbach 2001 – online. http://www.fellbach.de/kommunalpolitik/jugendgemeinderat/Dokumentation_JGROnlinewahl.pdf. (Verifizierungsdatum: 16.09.2005).

Steinbeis-Transferzentrum Mediakomm [2001]:

Erfahrungsbericht. (Online-) Jugendgemeinderatswahl in Esslingen am Neckar. http://www.wahlkreis300.net/fgiw/uploader/data/Esslingenbericht.pdf. (Verifizierungsdatum: 16.09.2005).

Steiner, Jens [2005]:

Digitale Republik Estland. http://www.politik-digital.de/egovernment/international/dibs_DigiRepEstland.shtml. (Verifizierungsdatum: 16.09.2005).

The Electoral Commission [2003a]:

Pilot scheme evaluation – St Albans City and District Council. http://www.electoralcommission.org.uk/files/dms/StAlbans_PartA_10212-8261__E__N__S__W__.pdf. (Verifizierungsdatum: 16.09.2005).

The Electoral Commission [2003b]:

Pilot scheme evaluation – Swindon Borough Council. http://www.electoralcommission.gov.uk/files/dms/Swindon_PartA_10221-8270__E__N__S__W__.pdf. (Verifizierungsdatum: 16.09.2005).

The National Election Committee [2004]:

General Description of the E-Voting System. Talinn: http://www.vvk.ee/elektr/docs/Yldkirjeldus-eng.pdf. (Verifizierungsdatum: 16.09.2005).

T-Systems CSM [2002]:

Onlinewahlen T-Systems CSM - Abschlussbericht der elektronischen Wahlen zum Betriebsrat bei T-Systems CSM im Mai 2002. http://www.wahlkreis300.net/fgiw/uploader/data/Wahl_CSM.pdf. (Verifizierungsdatum: 16.09.2005).

Vogt, Martin (Hrsg.) [1997]:

Deutsche Geschichte - Von den Anfängen bis zur Gegenwart. Fischer Taschenbuch Verlag: Frankfurt a.M..

Weixner, Bärbel Martina [2002]:

Direkte Demokratie in den Bundesländern - Verfassungsrechtlicher und empirischer Befund aus politikwissenschaftlicher Sicht. Leske + Budrich: Opladen.

Welz, Hans-Georg [2002]:

Politische Öffentlichkeit und Kommunikation im Internet. Bundeszentrale für politische Bildung: Bonn.

Wild, Michael [2003]:

Die Gleichheit der Wahl - Dogmengeschichtliche und systematische Darstellung. Duncker und Humblot: Berlin.

Will, Martin [2002]:

Internetwahlwahlen - Verfassungsrechtliche Möglichkeiten und Grenzen. Richard Boorberg Verlag: Stuttgart.

Wiltner, Frank [2003]:

Bedrohungen für Unternehmen. In: Gora & Krampert [2003], S. 81-96.

Winkel, Olaf [2004]:

Zukunftsperspektive Electronic Government. Aus Politik und Zeitgeschichte B 18/2004. Bundeszentrale für politische Bildung: Bonn.

Wobst, Reinhard [2003]:

Harte Nüsse - Verschlüsselungsverfahren und ihre Anwendungen. http://www.heise.de/security/artikel/39275/0. (Verifizierungsdatum: 16.09.2005).

Woyke, Wichard [1998]:

Stichwort: Wahlen - In Parlamenten, Bundesrepublik Deutschland, Frankreich, GB, USA, Europawahl. Leske + Budrich: Opladen.

Zippelius, Reinhold [2003]:

Allgemeine Staatslehre. Beck Juristischer Verlag: München.

Abbildungsverzeichnis

Abbildung 1: Typologien des E-Votings 25
Abbildung 2: Symmetrische Verschlüsselung [Fuhrberg 2000, 84]..... 51
Abbildung 3: Asymmetrische Verschlüsselung [Fuhrberg 2000, 90]. 52
Abbildung 4: Technischer Ablauf eines Wahlsystems. 64
Abbildung 5: Aufbau des schweizerischen Wahlsystems [L'Etat de Genève 2005]. 69
Abbildung 6: Aufbau des estnischen Wahlsystems [The National Election Committee 2004, 10]. 78
Abbildung 7: Zustimmung zur Internet-Stimmabgabe bei Wahlen [Hanßmann 2003, 226]. 92
Abbildung 8: Einführungsebenen des E-Votings. 108

Eigenständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und ohne fremde Hilfe verfasst und keine anderen als die angegebenen Hilfsmittel benutzt habe. Außerdem versichere ich, dass die Arbeit noch nicht veröffentlicht oder in einem anderen Prüfungsverfahren als Prüfungsleistung vorgelegt wurde.

Hildesheim, im September 2005

_____